UTS UNIVERSITY OF TECHNOLOGY SYDNEY

The evaluation of forensic intelligence to better understand the criminal environment for Australian document fraud

by Ciara Jean Devlin

Thesis submitted in fulfilment of the requirements for the degree of

Doctor of Philosophy

under the supervision of Associate Professor Scott Chadwick, Dr Sebastien Moret, Dr Simon Baechler, Dr Jennifer Raymond and Associate Professor Marie Morelato

University of Technology Sydney
Faculty of Science

September 2024

Certificate of Original Authorship

I, Ciara Jean Devlin, declare that this thesis is submitted in fulfilment of the requirements for the award of Doctor of Philosophy, in the School of Mathematical and Physical Sciences in the Faculty of Science at the University of Technology Sydney.

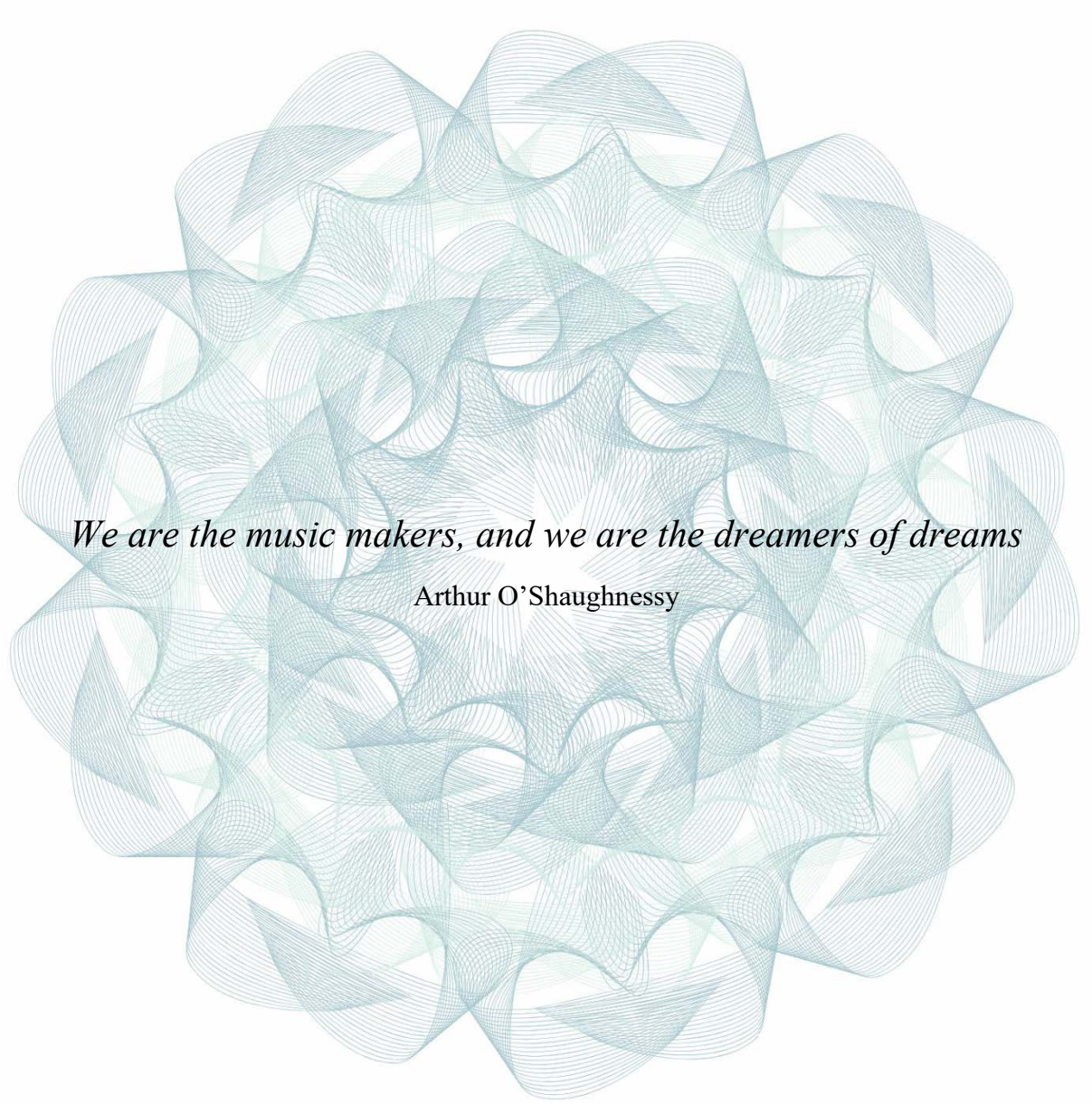
This thesis is wholly my own work unless otherwise referenced or acknowledged. In addition, I certify that all information sources and literature used are indicated in the thesis.

This document has not been submitted for qualifications at any other academic institution.

This research was supported by an Australian Government Research Training Program (RTP) Scholarship doi.org/10.82133/C42F-K220.

Signature: Production Note:
Signature removed prior to publication.

Date: 24/09/2024



We are the music makers, and we are the dreamers of dreams

Arthur O'Shaughnessy

Acknowledgments

I would like to begin by giving the most heartfelt and appreciative thanks to my UTS supervisors, Dr Marie Morelato, Associate Professor Scott Chadwick and Dr Sebastien Moret (yes Seb, I am still in denial about your leaving).

Scott, I can say in all honesty that if you had asked me six years ago what I was planning to do with my life, I would have never replied with "doing a PhD". In those two years after honours, the number of times that I ended up in your office telling you all about my next hair-brained scheme for my life, from psychology, criminology, all the way through to creative writing and arts, I remember you patiently listening and expressing your support (and disgust in the case of the arts plan) and telling me that if I left and decided to come back there would always be a place for me. I feel like even then you knew that this is where I would end up, and you were just patiently waiting for me to figure it out. You have been an incredible support, colleague and friend through this academic journey, and you have also helped me figure out a career path that I am excited to properly embark on. Without your support, guidance, and sarcastic remarks I know I wouldn't be where I am today, so thank you, most sincerely, it has been an honour. But also, I hope you don't let this go to your head.

Seb, I remember our first interaction in Complex Cases when I was doing my honours degree, and I honestly thought you couldn't stand me. It took me a little while to realise that you expected a lot from your students, and that it took some time to earn your respect. While it seemed that over time you started to warm to me, it wasn't until I started teaching for you in Forensic Imaging that I knew I had made it. Thank you for your kindness and guidance in helping me figure out that I wanted to keep learning. Your support has been greatly appreciated, and I will always be devastated that you moved overseas.

Marie, there were many times during 2018 that both Scott and Seb suggested I go and talk to you. Given my inexplicable aversion to lab work and love of analysis and writing they thought that forensic intelligence would be a perfect fit for me. I had no idea that suggestion would lead me to meeting and building such a supportive, wholesome, and beautiful friendship with one of the strongest and most inspiring women I have known. You have been such an incredible support, both academically and professionally, while also creating an environment where I can be upfront and honest about what is going on in my life and where I am at mentally and emotionally. That foundation of honesty, while sometimes blunt (which is one of my favourite things about you) has become so important to me, and it is something that I know I will take with me and try to emulate in my career with my (hopefully) future research students.

The three of you are incredibly important to me, and I will be forever grateful for everything you have done, all the (excessively long) drafts you have read, all the times you have told me, kind-heartedly to reel it in, and all the laughter and jokes we have cracked. You have created an incredibly positive, and warm PhD experience, and I know that I am very lucky to have had you as supervisors.

To my external supervisor from NSWPF Jen, you are an absolute rock star, and I am in awe of all the things that you have accomplished in your career. It has been an honour to work with you, and I appreciate how determinedly you emailed, called, and chased up any potential lead for more documents. As well, thank you for your advice and feedback on my chapter drafts, papers and presentations. I hope we can continue to work together into the future.

Simon, thank you for collaborating with me, and for taking time while I was in Switzerland to work with me, as well as to show me around the UNIL campus. It has been very rewarding getting to work with you, and I appreciate you finding the time to still have meetings, provide

guidance and help whenever you could, even with a significant time difference. I truly am sorry for the number of times you had to have 6am meetings with us.

This work would not have been possible without the generosity of my external partners. Thank you to the NSWPF stations that let me rummage through the documents you had on hand, as well as the stations who sent me documents to process. To Tracey, Emma, and Geoff, I am so grateful to the three of you for sending me the documents that you did. Not only taking the time to find those documents but also taking the time to redact them. Without a doubt, my work would not have been completed without your generosity. Thank you, and a special shout out to Geoff for putting up with my many "Hi, just checking in emails", you are an absolute gem of a human.

The third chapter of this thesis, focussing on the examination of the cryptomarkets would not have been possible without Associate Professor Quentin Rossy from the University of Lausanne, Switzerland. I will be forever grateful for your generosity in providing the cryptomarket data. My thesis was not initially going to swerve into the cryptomarket space, but when I started struggling to get access to documents, your data saved the day. Thank you, not only for the data, but also for reviewing and assisting in the cryptomarket side of my work, particularly in relation to the papers and presentations that I have given on that topic.

Now to my friends and family. I started my journey at UTS with my undergraduate degree in 2014, and little did I know that in one of the first lectures I would make a lifelong friend by picking a random girl to sit down next to. Ten years later, and having survived not only undergrad, but honours (and living together) and now PhD's, I know that I have found a friend for life in you, my dear Ana. I will be forever grateful for the unwavering support, kindness, advice and just all-around wholesome warmth that you exude at every moment of every day. You are one of a kind (and officially the only person who got a shout out in both my honours

and PhD acknowledgements – that's real love baby). I am so proud of everything you have accomplished and your incredible determination, I am looking forward to seeing where your career takes you next, and I am hoping that it isn't anywhere too far away.

Harry, I honestly had no clue when we first met that, firstly we would end up doing our PhD's together, but that you would also become such a crucial part of my support network at UTS. It has been such a pleasure getting to know you better and forming what is easily one of my favourite friendships. Thank you for always being supportive, and ready for early morning coffees, there were quite a few moments during this journey that those morning catch ups were all that kept me sane.

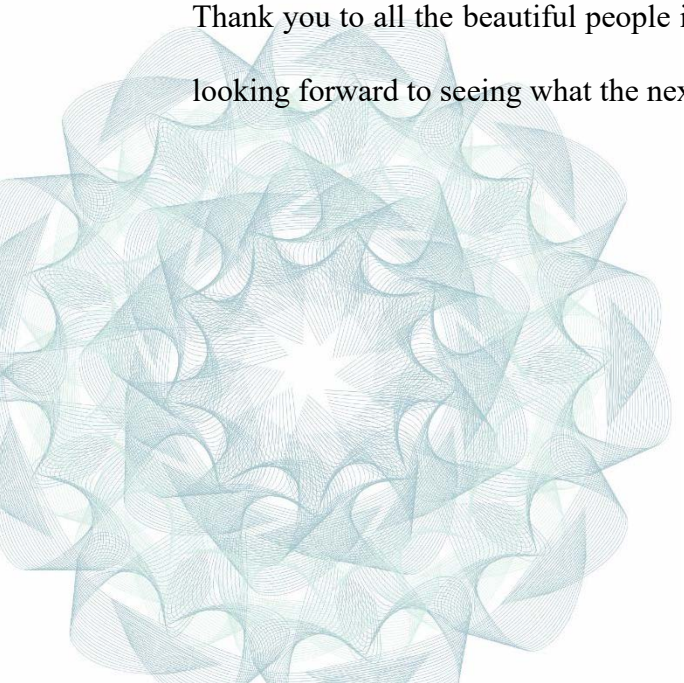
To the wonderful CFS PhD gang: Ana, Archie, Ayusha, Bridget, Eathan, Harrison, Harry, Layal, Macey, Matt, Mikki, Rachael, Rin, Samara, Sandi, Sharni, and Teneil, you are all so incredibly supportive and kind. Doing a PhD is such a complex and taxing experience, that can be hard for outsiders to understand. Having a support network of people who are traversing the nine circles of hell with you is so important, and I am glad that we have been able to brave it together.

To my family and friends who exist outside the PhD sphere, I want to thank you for your patience and support as I have slowly become more and more hermit-like as the PhD submission approached. To my dad, for reading every chapter of my thesis to not only show support but to help me catch those annoying typos that my brain would just skip over. To my mum, and my dear friend Liv for always listening to me brain dump and worry over the next deadline, experimental brick wall or writers block and for doing your best to be supportive and provide a comforting word. And to my friend Narelle, for offering to review and showing genuine interest in my thesis and the work that I have spent the last four years on. Your feedback was so valuable, not only to help me ensure that it could be understood by someone

outside of my very niche field, but you also helped me to believe again in what I was doing. So, thank you, sincerely.

Doing a PhD is known to be one of the most stressful and intense academic ventures a person can undertake. It can be easy to forget that on top of working through the PhD, life continues to happen, and that it is not always easy. During my PhD, I went through some significant life changes, loss, and grief, but also a huge amount of healing. Everyone in my life contributed to that metamorphosis, including my supervisors Scott and Marie, my friends and my family. But the person who helped me the most through so much laughter, joy, support, patience, and love, was my partner, Connor. Thank you for helping me stay motivated, especially over the last few months when the exhaustion and burn out began to loom on the horizon, reminding me to drink water and eat when the hyper fixation would take over, and letting me know that it was okay to take a break, cry, or just stare into the abyss if I needed to. And for providing me with emotional support cheeseburgers whenever they were requested. Since we met, my life outside of my PhD and my career has become so full, I have been welcomed into families, built from friends and from blood, and you have helped me to see that work is not the most important part of life. I will always love what I do, and I will always be immensely proud of the things that I have accomplished, especially this PhD, but I now know that there is more to life, and that my worth isn't dictated by my academic accomplishments. They are just a part of my story.

Thank you to all the beautiful people in my life that have been on this journey with me, I am looking forward to seeing what the next chapter brings.



Statement and list of publications

The publications below have been incorporated into the specified chapters.

Chapter 1 and 2

1. **Devlin, C.,** Morelato, M., & Baechler, S. (2024). Forensic intelligence: Expanding the potential of forensic document examination. *WIREs Forensic Science*, e1528. doi:https://doi.org/10.1002/wfs2.1528

Chapter 2

2. **Devlin, C.,** Chadwick, S., Moret, S., Baechler, S., Raymond, J., & Morelato, M. (2022). The potential of using the forensic profiles of Australian fraudulent identity documents to assist intelligence-led policing. *Australian Journal of Forensic Sciences, 55*(6), 720-730. doi:10.1080/00450618.2022.2074138

Chapter 3

3. **Devlin, C.,** Chadwick, S., Moret, S., Baechler, S., Rossy, Q., & Morelato, M. (2024). Illuminating the dark web market of fraudulent identity documents and personal information: An international and Australian perspective. *Forensic Science International 2024*:363(112203). doi:https://doi.org/10.1016/j.forsciint.2024.112203

Signatures of contributing authors

The signatures of all authors who contributed to the papers listed above have been included below.

Dr Marie Morelato

Signature: Production Note: Signature removed prior to publication. Date: 28/08/2025

Dr Scott Chadwick

Signature: Production Note: Signature removed prior to publication. Date: 28/08/25

Dr Sebastien Moret

Signature: Production Note: Signature removed prior to publication. Date: 28/08/2025

Dr Jennifer Raymond

Signature: Production Note: Signature removed prior to publication. Date: 28/08/25

Dr Simon Baechler

Signature: Production Note: Signature removed prior to publication. Date: 28.08.2025

Dr Quentin Rossy

Signature: Production Note: Signature removed prior to publication. Date: 28.08.2025

Conference presentations, invited talks, and awards arising from this thesis

Devlin, C., Chadwick, S., Moret, S., Baechler, S., Raymond, J., Morelato, M. (2021). *The potential of using the profiles of fraudulent identity documents to assist in intelligence-led policing*, Australasian Society of Forensic Document Examiners (ASFDE) INC Annual Scientific Meeting**,** Online, 24-28 May 2021

Devlin, C., Chadwick, S., Moret, S., Baechler, S., Raymond, J., Morelato, M. (2021). *The potential of using the profiles of fraudulent identity documents to assist in intelligence-led policing*, ANZFSS Research in the Spotlight**,** Online, 16th July 2021

Devlin, C., Chadwick, S., Moret, S., Baechler, S., Raymond, J., Morelato, M. (2022). *The potential of using the profiles of fraudulent identity documents to assist in intelligence-led policing*, European Academy of Forensic Sciences (EAFS) 2022*,* Stockholm, Sweden, 30th May – 3rd June 2022

Devlin, C., Chadwick, S., Moret, S., Baechler, S., Raymond, J., Morelato, M. (2022). *The potential of using the profiles of fraudulent identity documents to assist in intelligence-led policing*, 25th International Symposium, ANZFSS 2022*,* Brisbane, Australia, 11-15 September 2022

Awardee: Best Oral Presentation – Document Examination

Awardee: ANZFSS Executive Travel Scholarship

Devlin, C., Chadwick, S., Moret, S., Baechler, S., Raymond, J., Rossy, Q., Morelato, M. (2022). *Understanding the Australian fraudulent document market on an anonymous online dark web marketplace*, 25th International Symposium, ANZFSS 2022*,* Brisbane, Australia, 11-15 September 2022

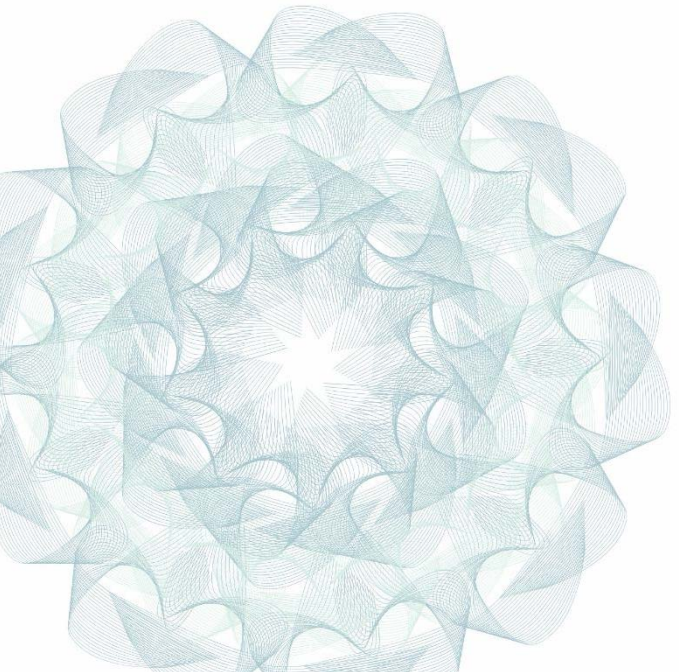
Awardee: ANZFSS Executive Travel Scholarship

Devlin, C., Chadwick, S., Moret, S., Baechler, S., Raymond, J., Rossy, Q., Morelato, M. (2023). Understanding the Australian fraudulent document market on an anonymous online dark web marketplace, *IAFS 2023,* Sydney, Australia, 20-24th November

Awardee: Bryan Found Memorial Award (ANZFSS Victorian Branch)

Devlin, C., Chadwick, S., Moret, S., Baechler, S., Raymond, J., Morelato, M. (2023). The potential of using the profiles of fraudulent identity documents to assist in intelligence-led policing, *FOSTER 2023,* University of Technology, Sydney, 1st December 2023

Table of Contents



List of tables

List of figures

List of abbreviations

ABS	Australian Bureau of Statistics
ACCC	Australian Competition and Consumer Commission
ACE	Analysis, comparison, and evaluation
ACIC	Australian Criminal Intelligence Commission
ACORN	Australian Cybercrime Online Reporting Network
ACPR	Australasian Centre for Policing Research
ACT	Australian Capital Territory
AFIS	Automated Fingerprint Identification System
AI	Artificial Intelligence
AIC	Australian Institute of Criminology
API	Application programming interface
ATO	Australian Taxation Office
AUD	Australian Dollars
BDM	Births, Deaths, and Marriages
BIDIF	Interstate Database of Fraudulent Identity Documents
CALD	Culturally and linguistically diverse
CEPOL	Collège Européen de Police
CIA	Central Intelligence Agency (USA)
CTSOCC	Commonwealth Transnational, Serious, and Organised Crime Centre
DDL	Digital driver licence
DDoS	Distributed Denial of Service
DFAT	Department of Foreign Affairs and Trade
DHS	Department of Human Services
DMV	Department of Motor Vehicles

DNA	Deoxyribonucleic acid
DOB	Date of Birth
DPI	Dots per Inch
DSLR	Digital Single-Lens Reflex
DVS	Document Verification Service
EDRS	Ecstasy and Related Drugs Reporting System
ELINT	Electronic intelligence
EMP	Empire Market
EUR	Euro
FCA	Formal Concept Analysis
FDE	Forensic Document Examiner
HPLC-QToF	High-performance liquid chromatography – quadrupole time of flight mass spectrometry
HTML	Hyper-text markup language
HTTP	Hyper-text transfer protocol
HUMINT	Human intelligence
HVP	High visibility policing
ICT	Information and communications technology
ID	Identity document
IDRS	Illicit Drug Reporting System
IELTS	International English Language Testing System
IIFMS	INTERPOL Forensic Science Managers Symposium
ILP	Intelligence-led policing
IMINT	Imagery intelligence
ISF	Internal Security Fund

ISP	Internet service provider
M.O.	Modus operandi
MLA	Mutual legal assistance
NCA	National Crime Agency
NCIS	Nation Crime Intelligence Service
NSW	New South Wales
NSWPF	New South Wales Police Force
NT	Northern Territory
NY	New York
OAIC	Office of the Australian Information Commissioner
OMCG	Outlaw Motorcycle Gang
OSINT	Open-source intelligence
OVD	Optically variable device
PGP	Pretty Good Privacy
POI	Proof of identity
ProFID	Profiling fraudulent identity documents
PSD	Photoshop file format
QLD	Queensland
QR	Quick Response
RBDM	Registry of Births, Deaths, and Marriages
ROI	Regions of interest
SA	South Australia
SIFT	Scale-Invariant Feature Transform
SMH	Sydney Morning Herald
SNA	Social Network Analysis

SWANA	Southwest Asia and North Africa
TAS	Tasmania
TNYT	The New York Times
TSOC	Transnational, serious, and organised crime
U.K.	United Kingdom
UNIL	University of Lausanne
UNODC	United Nations Office on Drugs and Crime
US	United States
USD	United States Dollars
UTS	University of Technology Sydney
UV	Ultra-violet
VIC	Victoria
WA	Western Australia
WHM	White House Market

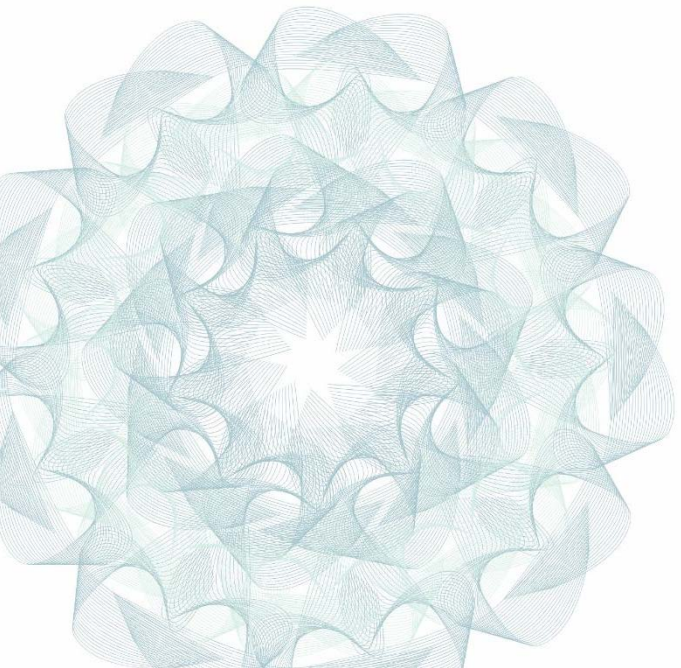
Ethics

All parts of the research conducted as part of *Chapter 2: The forensic profiling of fraudulent identity documents* was approved by the University of Technology Sydney (UTS) Human Research Ethics Committee (HREC) under approval ETH204695. All documents that were physically examined and collected were imaged, redacted, and saved in accordance with this ethics approval, ensuring no identifiable personal information was retained by the researcher. All digital images provided by external partners were redacted prior to them being sent.

The crawling and collection of the data that was used in *Chapter 3: The investigation of the online Australian document market* was in accordance with ethics approval granted by the University of Lausanne (UNIL), Switzerland (C_FDCA_022022_00009). This data was collected by an external UNIL collaborator and then sent for analysis. No identifiable, or personal information was collected during this data collection process, and all usernames presented in this work have been anonymised. By its nature the cryptomarkets ensure the anonymity of its users, so this research posed no risks to those individuals that had been using the cryptomarkets.

Funding

This research was supported by the Australian Government Research Training Program and UTS.



Abstract

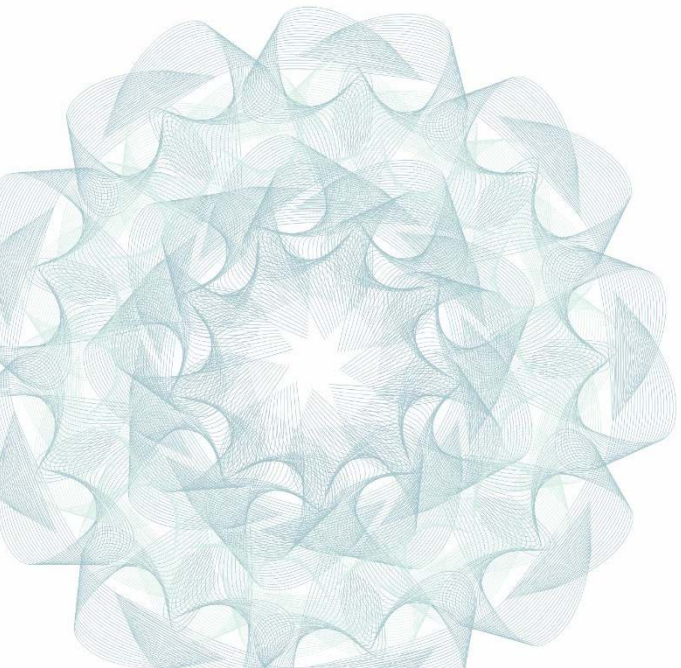
Identity crime and document fraud are pervasive and prolific problems that significantly impact individuals, communities, and governments. External to the direct impacts of these criminal environments, they are also known to enable and facilitate transnational, serious, and organised crime, including but not limited to the trafficking of illicit goods, human trafficking, and terrorism. Despite the harms caused by these criminal environments, and the fact that identity crime is considered the fastest growing criminal problem in Australia, very little is known about Australian identity crime and document fraud, largely due to the reliance on reactive reporting and policing methods.

To address this significant information gap and gain greater insight into the overall criminal environments for identity crime and document fraud, the market for fraudulent documents and personal information has been examined through the analysis of both the physical and digital traces of the market. This has been done in two parts, focussing on the visual profiling and comparison of 183 fraudulent identity documents collected from Australian law enforcement, and then the analysis of the ID-related market on two cryptomarkets (a.k.a. anonymous online marketplaces).

From the profiling portion of the work, it was identified that 94% of the documents were linked to at least one other document, and 17 series emerged, the largest of which contained 54 documents. Therefore, suggesting that the physical side of the market for fraudulent documents within Australia is likely organised and that there are prolific offenders contributing a disproportionately large number of products to the market. This level of organisation was also identified within the digital side of the market, with a small number of vendors (13) contributing 63% of the sales to the ID-related market. Through the analysis of the products available, their supply, demand and trafficking patterns, it was possible to identify that

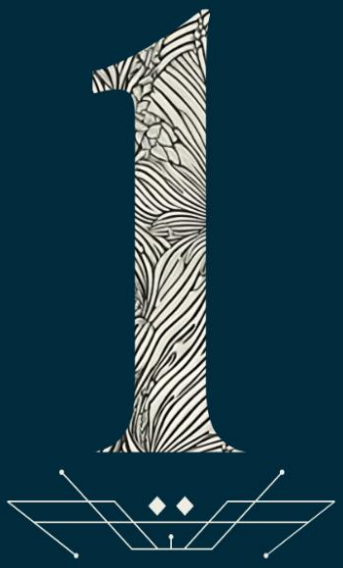
Australian documents were the second most listed and sold products, and that both the U.S. and Australia appear to have largely domestic markets. These analyses provide valuable information, both illuminating an often-shrouded illicit marketplace, as well as providing extra insight that can assist intelligence-led policing.

Currently within Australia there are many siloes between the different organisations and research bodies that deal with identity crime and document fraud. This research illustrates that not only is a combined analysis of both the physical and online portions of the market required to understand the criminal environment for document fraud and identity crime, but that more information sharing and collaboration is required between the organisations that work within the identity crime space. Only through the active sharing of identity crime reports, document seizures and survey-based research in combination with the monitoring of both the physical and digital portions of the market will it be possible to holistically understand the criminal environments of identity crime and document fraud, and therefore more proactively police it.



s

Chapter



Introduction

1 Introduction

Traditionally, the main function of forensic science has been to assist in solving cases within the judicial system, largely through identifying the relationships between traces and their putative sources [1-4]. While undoubtedly crucial, this almost tunnel-visioned, reactive approach towards the criminal environment has proven to be inefficient and ill-equipped to cope with larger-scale organised criminal networks and serial offenders [5, 6]. Research over the last fifteen to twenty years has clearly illustrated how the contribution of forensic science can be broadened to have a greater impact on crime rates and to foster a greater understanding of the criminal environment [2-4, 7-10]. While much of this has had a focus on the illicit drug market, this research will focus on the criminal environment of identity crime, more specifically that of fraudulent identity documents, building upon work that has been conducted overseas, most notably in Switzerland [11-19]. It will illustrate how fraudulent identity documents as a type of trace have been underutilised within Australia, and how their physical examination and profiling, along with the interrogation of their supply chains can be used within a multi-source approach to provide quality intelligence to help understand the criminal environment of document fraud, and identity crime, within Australia. This work is split into four sections, this first section, Chapter 1, introduces general background information relevant to all parts of the thesis. The second section, Chapter 2, focuses on the investigation into a systematic forensic profiling method for fraudulent Australian identity documents, assessing how these profiles can be used to gain insight into the criminal environment and providing recommendations for how the systematic model used internationally could be implemented domestically [15, 16]. The third section, Chapter 3, includes an investigation into the fraudulent identity document market on anonymous online marketplaces also known as cryptomarkets. This section examines the supply and movement of these documents through the dark web, highlighting trends in the supply, demand, and trafficking of these documents. The final

section, Chapter 4, examines how together, these two seemingly separate data sources, in combination with alternative information from a range of sources can provide a clearer picture of the criminal environment of identity document fraud and thus identity crime within Australia, and how this can assist intelligence-led policing.

1.1 Identity-related crime

1.1.1 Identity and its value

The word ‘identity’ has a broad range of meanings and connotations across a variety of fields, with common definitions spanning psychology, philosophy, sociology, and law [20, 21]. Within this research, an individual's identity is considered to be a combination of characteristics that enables the individual to be distinguished from all others [22], whether that be in the physical or digital world [21]. Depending on the context of the situation, and what level of identity proof is required, it is possible to prove one’s identity through the use of a range of different ‘types’ of identity, being biometric, attributed, biographical, and chosen [23, 24].

> ***Biometric identity*** refers to those identity proofs that are intrinsically linked and unique to the individual such as fingerprints, DNA profile (except for identical twins), and retinal scans. [24].
>
> ***Attributed identity*** refers to identity elements that the individual receives as a result of their birth such as their name, date and place of birth, and parental information. It also includes governmentally bestowed identifiers that the individual collects over the course of their life such as ID numbers [24].
>
> ***Biographical identity*** refers to those elements that an individual collects over the course of their life (due to choices) such as marriage certificates, employment history, education and degrees, and insurance policies. [24].
>
> ***Chosen identity*** includes characteristics that an individual selects over the course of their life and includes things such as passwords, nicknames, usernames, gender identity and pronouns [23].

In Australia, an individual's identity is generally accepted as being established at birth through the generation of a Registry of Births, Deaths, and Marriages (RDBM) birth record or certificate that includes unique information about that person [22]. Similarly, for those individuals that are not born on Australian shores, their identity in Australia is usually established from personal details recorded on their immigration documents [22]. These documents, along with other types of identity information (listed above) are combined to form an individual's legal identity, being that which is recognised by the governing structure of a country. To ensure individuals can prove their legal identity, governments issue official and secure documents that include the basic information required to attest to the identity and status of the individual who holds the document [21].

The ability to prove one's legal identity is a cornerstone of many aspects of modern social and economic life, as it dictates their access to a range of entitlements and resources such as government benefits, financial institutions, security, housing, health care, travel, and the ability to work [21, 25]. Social, political, and economic aspects of society are built upon the ability for organisations, institutions, and governments to verify the legal identity of an individual [21]. Very early legal systems were able to identify individuals solely through their first or last name, however, this was only successful while the population remained more or less static [21]. With increases in populations, globalisation, mobility, and digital technologies, the need for reliable and detailed identifiers has only increased [20]. Now, the ability to prove our (legal) identity relies on our possession of identity and travel documents, often termed secure documents due to their embedded security features meant (1) to prevent or hamper illegal replication or manufacture, and (2) to enable the assessment of their authenticity [26-28].

Understandably, the value associated with identity, and the documents required to prove it, has resulted in an expansive criminal environment focused on the theft, manufacture, and misuse of identity information, also known as identity crime. Through the illegal use of another

person’s identity, whether it be of a real or fictitious person, one can gain access to a range of benefits. This type of information can even be used to facilitate other crimes such as theft and fraud along with organised crime and terrorist activities [29-32].

1.2 Identity crime, theft, and fraud

Throughout the literature along with international and domestic statutes and laws, there is no generally accepted definition used to describe identity-related crimes. Across jurisdictions, these crimes can be classed as identity fraud, identity theft, or the more generic term identity crime [29, 30, 33]. This creates issues when trying to understand, research, and even prosecute within this criminal environment. For clarity, within this research the following definitions from the Australasian Centre for Policing Research (ACPR) have been applied, and it is believed that these are the definitions that are gradually being applied within the policing of identity crime within Australia [33].

> ***A false identity*** may be established through the fabrication, manipulation or theft of a pre-existing identity, whether that be an individual (living or dead) or a corporation or company [33].
>
> ***Identity fraud*** refers to the use of a false identity in order to gain money, goods, services or other benefits such as welfare, medical care or to facilitate things such as tax evasion [33].
>
> ***Identity theft*** involves the theft, or use of a pre-existing identity without, or sometimes with the consent of the lawful user of the identity. This is often the first step towards committing a form of identity fraud. The use of the term 'theft' to describe this criminal behaviour is somewhat of a misnomer and can cause issues when trying to prosecute crimes of this type [21, 34]. In Common Law theft is considered to be the theft of tangible property, with the requirements of it being the removal of the property from the possession of the victim, without their consent, and with the intent, on the part of the perpetrator, of permanently removing the property from the possession of the victim [34]. In the case of identity theft, none

of these parts of traditional theft are satisfied. In most cases the identity information or document is not removed from the victim, instead a second person assumes their identity and begins using it simultaneously [33-35].

Identity crime is a broad definition that is used to describe offences in which a perpetrator uses a false identity in order to facilitate the commission of a crime, encompassing all offences that are facilitated by or rely upon the use of identity information and documents [36]. This includes the acquisition, production (i.e. manufacture and/or manipulation), possession, transfer (i.e. trafficking) and/or use of identity information or documents [21, 29]. The possession of document precursors and equipment used to store or manufacture these documents (i.e. templates, computer files, security features, card printers etc.) is also included as part of this definition [21]. While the use of false identities is most commonly linked to types of fraud, false identities have been known to facilitate a broad range of organised crime and terrorist activities such as money laundering, child exploitation, human trafficking, and the trafficking of illicit goods [29, 32, 33].

1.2.1 Document fraud and identity crime

The ability to commit an identity crime, in most cases relies on the ability of the offender to prove their false identity, a key part of which relies on the use of fraudulent identity documents. As discussed above, proof of identity documents hold a great deal of power, which has resulted in a strong international market for fraudulent identity documents being established. While originally these documents began as simple pieces of paper with printed information, due to advancements in both technology and the skills of illicit manufacturers, more secure documents have been developed to try and dissuade the criminal environment for fraudulent documents [26-28]. However, as the value behind these documents and the number of benefits they afford has increased, so too has the desire to produce, distribute, and use fraudulent versions [37, 38].

The expansion of criminal enterprises has similarly resulted in the development of several different types of fraudulent documents, with the most often encountered including counterfeit documents, forged documents, and pseudo (or fantasy) documents [25, 39-43]. The terminology behind these documents is summarised in Table 1.1. These definitions are based on the methods, or modus operandi (M.O.) used by the forger(s) to create or alter them.

Table 1.1: Main security document terminology and definitions as a consensus from various sources [25, 39-43].

Fraud type	**Definition**
Counterfeit	A completely unauthorised and illegally manufactured reproduction of a genuine document that includes features that attempt to replicate the security features seen in a legitimate version
Forgery	A genuine document that has been partially altered to give misleading information (e.g. substituted photograph, addition of a vehicle category, erasure of an expulsion stamp)
Pseudo (a.k.a fantasy) document	A manufactured document that is not officially recognised by any authority, it is often made to look like a legitimate document type
Stolen blank document	A document that was originally produced by an official authority, but then stolen and personalised by a forger

While a counterfeit or a pseudo document is manufactured from raw materials, a forgery is instead a genuine document that has been altered. Pseudo documents differ from the other two types, in that these documents are not officially recognised by any authority, this could be a document claiming to originate from a completely fictitious country, or it could be a completely fictitious document type from a legitimate country [40, 43]. These documents will often have

the appearance of a legitimate identity document, and are often those marketed as ‘novelty items’ [43]. An example of a fantasy document is shown in Figure 1-1. It has been manufactured to look like a non-restricted Australian driver licence from New South Wales (NSW), however a ‘NSW Student Identification’ card is not an officially recognised document. For the sake of concision, M.O. that are beyond forensic interest have not been included here. This largely includes instances where the document itself is genuine, such as a legitimate document that was issued based on fraudulent information, or an impostor using the genuine document of someone else.

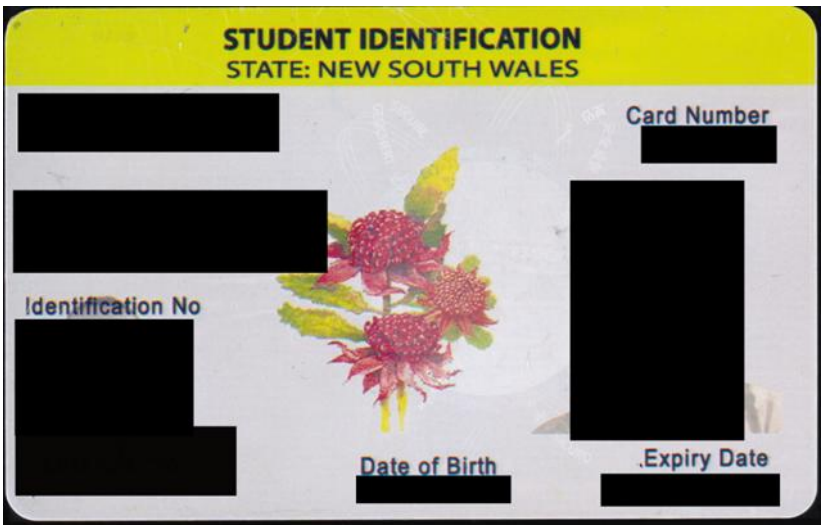


Figure 1-1: Example of a pseudo document seized in New South Wales, Australia

1.2.2 The criminal environment of identity crime

Throughout the literature there is a general consensus that identity crime is a serious problem that appears to be trending upwards, likely due to increases in digital technologies and online transactions [44, 45]. Between the years of 2013 and 2019 the percentage of respondents (to the Australian Institute of Criminology’s identity misuse survey) that had experienced the misuse of their personal information over the course of their lifetime remained fairly consistent between 20-25%, which increased to 31% in 2023 after a slight drop to 19% in 2020 [29-31]. Not only have the instances of identity crime been, for the most part, increasing, so to have the

costs associated with this criminal environment. Between 2018-19 the direct and indirect costs[1] of identity crime were estimated to be $3.1b, 17% more than the costs incurred within the 2015-16 year, even when considering the impact of inflation [29]. Identity crime is also increasingly impacting Indigenous Australians. The Australian Competition and Consumer Commission's (ACCC) ScamWatch report from 2022 illustrates that for Indigenous Australians monetary losses from identity crime showed a 239.3% increase from the previous year to $228,927 [46].

When trying to understand the criminal environment for identity crime, it becomes difficult to gather a clear picture given how many different government and research bodies focus on this crime type, all with varying results. It is estimated that 58% of fraud involves some element of identity misuse (Cifas, 2019 as cited in Franks et al. 2020 [29]). Franks et al. (2020) indicate that between 2018-2019 Australian police agencies reported 116,643 fraud and deception offences, so if the estimate of 58% is correct, there should have been approximately 67,523 identity-related offences recorded between 2018 and 2019 [29]. However, the ACCC states that from their ScamWatch reports[2] there were only 11,373 reports of identity theft in 2019, which subsequently increased by 84% to 20,000 in 2020 (ACCC, 2021a, as cited by McAlister et al. 2021 [31]). While the disparities between these different reports make it difficult to grasp a proper understanding of the extent of identity crime within Australia, the most significant barrier is that identity crime is significantly under-reported by victims, either knowingly or unknowingly [30, 31, 46], with approximately 70% of victims not officially reporting the misuse of their personal information [29]. This means that although there are numerous organisations working within the identity crime space, as they are largely reliant on the reactive

[1] Direct costs include losses suffered as a direct result of identity crime, such as those suffered by Australian businesses, individuals, and government agencies. Indirect costs are those incurred when trying to prevent or respond to identity crime. These are often due to law enforcement and other private sector prevention efforts [29].
[2] Generated on request through ACCC ScamWatch Scam statistics (https://www.scamwatch.gov.au/research-and-resources/scam-statistics)

reporting of crimes and seizures of documents, they are only capturing a portion of the overall criminal environment of identity crime. So not only is the identity crime problem likely far larger than currently reflected by these reports [44], it is likely to continue increasing as the years go on, with it previously having been described as the fastest growing criminal environment in Australia [45].

Of the portion of cases that are reported officially, an even smaller percentage of these result in any police investigation and subsequent prosecution [47]. If the Australian Bureau of Statistics' (ABS) estimate of 2.1 million victims of identity crime in the 2018-19 period is correct, then only 5.3% of these cases make their way through the judicial system to some form of resolution, whether that be a guilty verdict, acquittal, transfer or withdrawal (Australian Bureau of Statistics, 2020, as cited by Franks et al. 2020 [29]). Apart from the acknowledged under-reporting of identity crime, a potential reason for this low prosecution rate may be the difficulties associated with defining identity crime, and the lack of a consistent legal framework within which to prosecute these crimes. While most countries rely on more generic fraud, theft, or computer crime statutes to prosecute identity crimes, most states in Australia, the United States, and Canada all have statutes that specifically address identity-related crime [21]. However, they still lack the required consistency to properly address the cross-jurisdictional and borderless nature of identity crime as they all vary in the terms that they use, and their definitions, with each country using identity crime, identity theft, and identity fraud interchangeably.

Not only are there inconsistencies internationally, but even within Australian states there is significant variation in the statutes in place for dealing with identity crime [34]. While most states (QLD, NSW, WA, SA, NT, and VIC) have identity crime specific provisions in their statutes, the nature of what is considered an identity offence varies between these jurisdictions [20, 34]. Appendix Table A. 1 and Table A. 2 illustrate the five key aspects of identity crime

(production, acquisition, possession, transfer/trafficking, and use of identity information) along with the identity crime related provisions from the statutes of each Australian state. For those states that do not have identity crime provisions within their legal framework, such as Tasmania (TAS), the laws and statutes that are most used to prosecute identity-related offences have been included to contrast and illustrate the gaps within the legislation.

Most of the identity crime provisions within Australian statutes focus very heavily on the mental element of identity crime, including within their wording 'knowledge' and 'intent'. This requires the prosecution to prove that the offender knew the information was identity information, and that they had the intent to use that information to commit or facilitate a further crime [34]. From a legal perspective this makes sense, as simply possessing someone's credit card details does not constitute a crime. It only becomes a crime when the intent of the individual in possession of the credit card details changes. This can be near impossible to prove, resulting in prosecutions relying on confessions in cases where intent is unclear [34].

Further hampering the understanding of this criminal environment is that, by its nature, identity crime is borderless. Increases in globalisation and technology have created a digital ecosystem in which identity crime can flourish, making it far easier to take advantage of the fount of personal identification information that is stored, used, and made available online. Now, someone in the United States could purchase the identity information of an Australian individual through the dark web and then use that information to make purchases in Italy. So inconsistencies in the language, laws, and definitions used to encapsulate identity crime, makes it very difficult to conduct inter-jurisdictional comparisons and prosecutions [34, 47]. Further muddying the waters is the diverse range of reports, sources (such as police seizure information and victims), and institutes (such as the ACCC, Australian Institute of Criminology and ABS) conducting research into the identity crime environment, all using different data sources,

methods, and terminology. This has resulted in a criminal environment that is known to be expansive but ill-defined.

1.2.3 Addressing identity-related crime

In general, the strategies for combatting identity crime where existent are only partial, with each jurisdiction or country's strategies coloured by their specific concerns regarding this crime type. This lack of unified combat mechanism, or legal framework is surprising given the often trans-jurisdictional and international nature of identity crime. Instead, singular problems are addressed rather than fostering collaborative and proactive methods to try and help increase the understanding of the criminal environment and reduce instances of this criminality [23].

In most cases, identity crime is considered to be a crime of opportunity, however, the systematic use of identity information by organised crime networks [21, 37, 47], suggests that there may be the potential to use the concepts of forensic intelligence to help understand and proactively disrupt the criminal environment of identity crime. Organised crime activities are in most cases structured, systematic, and repetitive, providing opportunities to examine criminal behaviours to help identify links between cases, individuals, and organisations. This is especially true when considering that many types of identity-related crimes can be committed with very similar M.O. [15, 23]. This was illustrated by the ACCC in their use of intelligence to help combat scams (which often have an identity crime component) through their 2022 ScamWatch Report [46]. By examining trends in scam reports they were able to provide intelligence to law enforcement and government bodies and assisted in the investigation and prosecution of scammers that were operating within Australia [46]. This proactive method of dealing with scams illustrates the likely success associated with using a forensic intelligence method to assist in combatting the identity crime environment, especially given the similar format of these two crime types existing largely within the digital realm.

A key component of identity crime is the manufacture and use of fraudulent identity documents and credentials, of which document examination plays a key part. However, in most cases the focus within document examination (specifically relating to identity and security documents) is to simply determine the authentication status of a document i.e. whether it is genuine or fraudulent. While the detection of these fraudulent documents is a crucial first step in understanding the criminal environment of identity crime and document fraud, it reinforces the misconception that no further information of note can be gathered from a document once it is determined to be authentic or fraudulent. Currently, within Australia, one tool that has been developed to try and address the identity crime and document fraud problem is the Document Verification Service (DVS), facilitated by the Australian Government, which assists in the detection of false documents and information [48]. Organisations can use this online tool to verify their clients' identity documents against the original, government records, preventing enrolment or registration within their systems using false information [29, 48]. During the verification process, the information is sent via a secure communications pathway, returning a yes or no answer as to whether the records match [49]. While the number of organisations using the DVS has been increasing, it is still quite a reactive way to try and combat this criminal environment, with the offenders only being targeted when trying to use the identity that has already been stolen, assumed, or forged [15]. By only targeting this crime type at the point of use, the potential of targeting these offenders earlier on in the criminal enterprise is being neglected, resulting in there being very limited impacts on the criminal environment. Previous research has underlined that for identity crime to be properly addressed within Australia, coordinated efforts from both government and private sectors are required [30], and while the DVS is a good first step in this direction, it is only capturing a part of the criminal environment.

Generally, the examination of these security documents, and therefore their authentication, falls within the purview of not just forensic document examiners (FDE's), but also across a range

of in-house document expert units that have been created by specific organisations such as banks, border police, and customs officers [50]. These in-house teams exist outside the umbrella of 'forensic science', while still applying a forensic science approach to examining these security documents. However, in most cases, the sole aim of these examinations is to simply determine the authentication status of the document being examined, fitting firmly within the judicial paradigm and the case-by-case approach to policing.

Undoubtedly, the use of forensic document examination to assist in the resolution of cases is important, however, these traditional case-by-case approaches are not equipped to properly deal with the prolific and pervasive nature of identity crime and document fraud. The paradigm reinforced by the traditional judicial system structure greatly limits both the impact on and the understanding of the criminal environment of both document fraud and identity crime. Furthering this lack of impact is the variation in the extent of collaboration between these in-house document expert units and forensic science institutes. This results in the forensic examination of security documents being somewhat split between two professional communities that need to be more integrated, particularly to provide a proper understanding of this criminal environment and how it can be most effectively addressed.

It is clear that identity crime within Australia (and around the world) is a serious problem, that is continuing to increase [46]. Proactively addressing this criminal environment could assist in the identification and disruption of prolific identity crime offenders, thereby reducing the crime rate, but could also help to prevent other, more harmful crimes that are facilitated by identity crime and document fraud [32, 37, 46, 51]. Current attempts to manage this criminal environment are hampered by reactive, case-by-case approaches focussing on the authentication and detection of fraudulent identities and documents, with only those using the fraudulent information and documents being punished. A bigger picture attitude is required to properly understand this crime problem, and the best place to start is to consider the potential

of applying forensic science and forensic intelligence methods to facilitate a greater understanding of this criminal environment to help inform on more proactive ways to tackle it.

1.3 Intelligence and forensic intelligence

1.3.1 Intelligence-led policing (ILP)

Traditionally, policing has focused on reactive methods where cases are dealt with as they are reported. Officers perform their duties in reaction to calls or requests for services and conduct regular duties such as receiving complaints and randomly patrolling areas to illustrate their presence (including but not limited to high visibility policing, HVP) and looking for crimes that have occurred or are in progress [52].

While this is an effective method of resolving individual cases, an unrelenting rise in crime in the late 1980's and early 1990's called for police to become more proactive, efficient, and cost effective [53-55]. Simultaneously, increases in globalisation and advances in digital and communication technology [56] created more pathways and avenues through which organised crime could flourish [53]. It became clear that the traditional methods of policing were ultimately untenable, utilising a large amount of resources and time with little effect on the overall crime rate [5, 6].

This expansion of criminal activity across an international canvas illustrated the pitfalls of the traditional approach to policing. The emphasis on the crime itself as opposed to the offender often resulted in a large amount of resources and time spent to solve individual cases with little to no effect on overall crime rates [5, 6]. After research indicated that a small number of recidivists were responsible for a disproportionately large amount of crime [53, 57], there was a need to shift the policing paradigm, recommending that more resources be funnelled towards intelligence gathering and the proactive targeting of serious and prolific offenders [5, 57]. This

gave rise to what then became one of the central principles of intelligence-led policing (ILP), the proactive identification and targeting of the active criminal subpopulation [5] in order to reduce, disrupt and prevent crime "…through strategic management and effective enforcement strategies…" [58].

The aims of ILP can be identified through looking at the tactical tasking priorities of the United Kingdom (U.K.) National Intelligence Model [59] which was designed and distributed through the National Criminal Intelligence Service (NCIS), now superseded by the National Crime Agency (NCA). The aims of this model, accepted as the first real implementation of intelligence-led policing, aimed to actively target offenders, manage crime and disorder hot spots, investigate linked series of crimes and incidents, and apply preventative measures to reduce crime and disorder [53, 59]. The use of ILP, however, extends beyond just being a method through which to target prolific offenders and organised crime [52]. If implemented correctly, ILP can be a conceptual or management framework that can be used to successfully and more efficiently conduct the business of policing [5]. Focusing on intelligence as a foundation for identifying priorities and objectives, both strategic and operational, can more effectively prevent and suppress crime and other threats [52, 53]. This policing model also places a greater emphasis on the importance of information sharing and collaboration to address policing problems at both the local and regional level [60].

The successful integration of this policing model is dependent on more than just the possession of knowledge and intelligence [52]. In order to produce useful intelligence that decision makers can act upon, and thus bring about change, an intelligence framework (such as the intelligence cycle) is required to help collate, analyse, interpret, and disseminate the information [61, 62].

1.3.2 From ILP to the intelligence cycle

1.3.2.1 Intelligence as a concept

At the core of ILP, is 'intelligence' which as a concept, has remained enigmatic for many people [63], largely due to often inconsistent definitions. The term 'intelligence' has been used to simultaneously describe products, trends, methodologies, structures, and processes depending on the context [52]. For this research, the term intelligence is understood as the result of a process that turns raw, unintelligible data into a form that can be used in decision-making [1, 58, 64].

It is impossible to discuss the concept of intelligence without mentioning three key terms, data, information, and knowledge. These concepts all feed into one another and come together to form the overall picture of intelligence. The starting point is data, being raw uninterpreted observations or measurements [52]. This data can be gleaned from financial reports, customer information, or in the field of forensic science, case information and traces. This raw data is then put into context and given meaning through which it becomes information. The information when given an interpretation and understanding, can then become knowledge. Finally, intelligence is any data, information, and knowledge that has been evaluated, analysed, and presented to decision-makers for action-oriented purposes; this process is illustrated in Figure 1-2 [52].

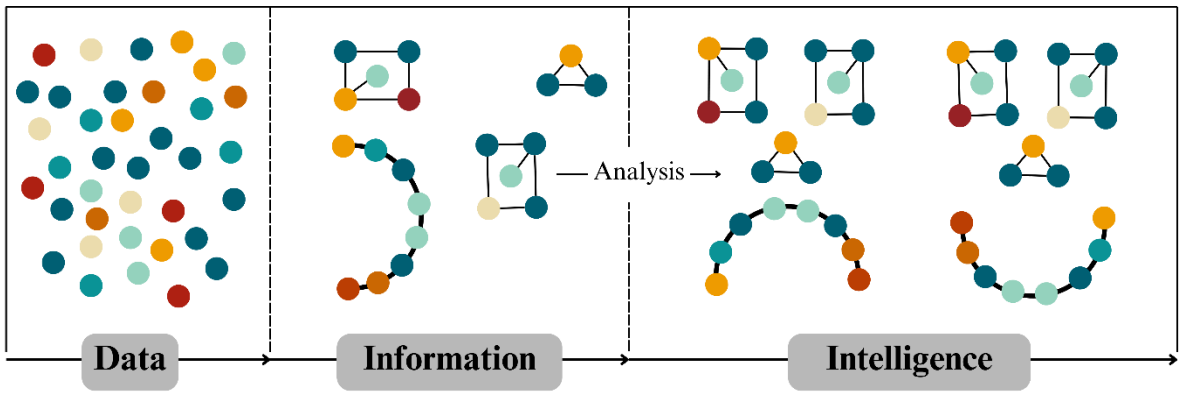


Figure 1-2: The intelligence process, with data becoming information and then intelligence adapted from Cartier, 2009 [65]

1.3.2.2 The intelligence cycle

The key to data, information, and knowledge becoming intelligence, is its ability to be effectively detected, collected, analysed, and communicated to decision makers or stakeholders in a timely manner, so they can take action and affect change where relevant [5, 64]. To accomplish this, most institutions implement what is known as the "intelligence cycle".

While one of the first uses of the term "intelligence cycle" can be traced back to 1948 [66], currently, the intelligence cycle is broadly used across organisational intelligence and in research. While all iterations of this model are described as an intelligence cycle, there is often some disparity between the terminology used and the number of steps included within the model. However, in all instances the model is described as a cyclical and iterative process comprised of at least six steps: including planning and direction, collection, evaluation and collation, analysis, dissemination, and re-evaluation. These steps will be explored in further detail below, with a simple visualisation of the intelligence cycle provided in Figure 1-3.

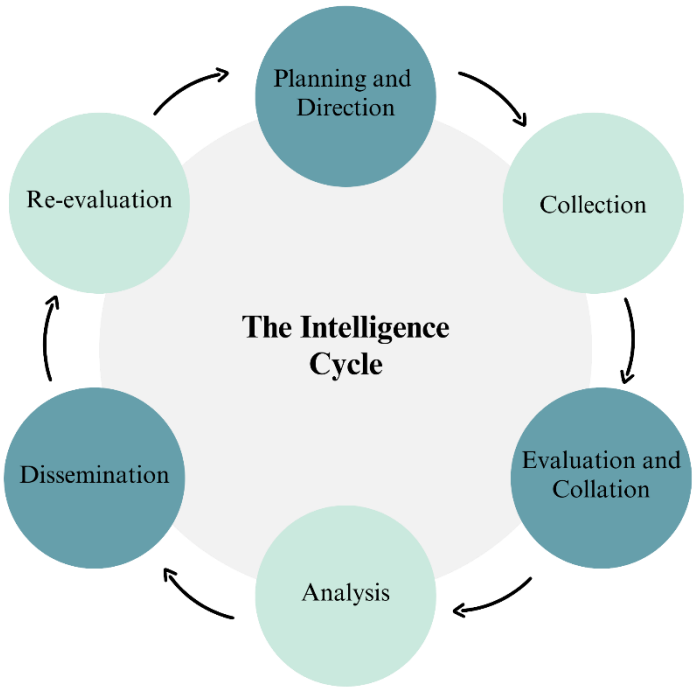


Figure 1-3: The intelligence cycle adapted from [72, 73]

***Planning and direction*:** This initial phase begins when a customer (most often a policy or decision maker) requests intelligence on a particular issue or target [67]. An assessment then takes place on the pre-existing data to determine what gaps need to be filled by further data collection and how this can be done efficiently, and legally [68].

Collection: Once the aim of the intelligence gathering has been indicated, collection of relevant raw data begins. This raw data can come from a wide range of sources such as traces, witness interviews, open-source information, photographs, and articles. It is common within contemporary intelligence to separate the sources of intelligence into subcategories or "INTs" outlined by the CIA to include electronic intelligence (ELINT), imagery intelligence (IMINT) which includes visual representations in any medium, human intelligence (HUMINT) which refers to intelligence derived from human sources and open source intelligence (OSINT) which is, as the name suggests, any form of publicly available information [67].

Evaluation and collation: The raw data collected is then evaluated and collated in preparation for the analysis step [67]. Through a close examination, the reliability and validity of the data source is determined, with any irrelevant or unreliable information being excluded. It is at this point in the cycle that data is converted into information. This information is then collated, combined with pre-existing information, and readied for analysis.

Analysis*:* It is during the analysis stage that the information is transformed into knowledge. By examining the information identified from the original data set along with the information that it was combined with during the collation phase it becomes possible to identify links and patterns and test hypotheses. This step is

crucial to the intelligence cycle, and is usually driven by a question, or goal, either explicitly stated by the customer, or implicitly anticipated by the analysts [1].

Dissemination: Lastly the intelligence created during the analysis phase is distributed to the decision makers or customers (those who requested the intelligence gathering in the first stage). To affect any real change, it is imperative that the intelligence is communicated in a timely manner, but also in a way that can be easily understood.

Re-evaluation: The memory, which is defined as all the information that the organisation has, at a certain time, about criminal activities, must be constantly updated and the intelligence produced is examined for its effectiveness at addressing the original problem at hand identified by the decision-makers or clients [67]. This process is then started all over again and any updated requirements from the decision makers are passed on to the data collectors [67] creating a cyclical process that is subject to constant feedback and re-evaluation.

Throughout the literature and operations, there is some disparity in the steps of the intelligence cycle, with some steps being combined, removed, or separated depending on the source. In practice, the generation and dissemination of intelligence is unlikely to follow such a clear linear or cyclical sequence of steps [69], as real-life operations are often more chaotic and needs based. However, this ideal representation of the intelligence cycle is a starting point that can, and often is, adapted to suit specific organisational or operational needs.

1.4 Forensic intelligence

Intelligence and the intelligence cycle, as mentioned previously, can be used across a range of different organisations, fields, and operations, including within forensic science and policing, with it being a core component of intelligence-led policing. Within this context, the term forensic intelligence describes the use of intelligence within the hierarchical framework of policing organisations, with a strong focus on using the intelligence to assist in the disruption, prevention, and reduction of crime or crisis management [58, 70] .

At its core, forensic intelligence is a different way of using traces, or remnants of criminal activity. Where forensic science has conventionally focussed on examining the features of a trace to elicit an answer or explanation relating to the source or activity behind its creation [1-4, 7], forensic intelligence has a larger scope, focussing more on the criminal activity itself to provide insights into the disruption, prevention, and proactive reduction of crime [58, 70]. The process relies on information collection, analysis, and interpretation and aims to assist decision makers (e.g. policing and government organisations) in affecting change [1].

Forensic intelligence aims to complement the more traditional reactive policing methods, acting on information gained through the traditional judicial approach, along with other detection routes (e.g. border seizures and bank clerks) in a more proactive way [1]. Expanding the possible routes of detection beyond the traditional limits of the judicial system enables a more objective, and thorough understanding of the criminal environment, especially those that may be difficult to infiltrate or understand through traditional means. Where previously a successful case might result in one conviction, the implementation of forensic intelligence would mean that the M.O. and traces collected from that scene could be examined and compared with other cases. Thus, highlighting possible similarities and potentially linking that perpetrator to multiple criminal acts (such as through the similarity of traces, or M.O.), or

identifying patterns in victimisation and the locations of criminal acts i.e. “hot spots”, being locations with high levels of repeat criminality.

All these observations can then be used to assist decision makers in actioning change that can reduce the overall scale of the criminal environment. Generally, crime is punctuated by prolific offenders and the concept of recidivism, meaning that those individuals committing a crime are likely to have done so in the past and to continue doing so into the future [1]. While this is a concerning thought in general, it also ensures that forensic intelligence can be wielded as a powerful tool against recurrent criminal activities. So, through the targeting of one repeated act of criminality (i.e. a prolific offender) it becomes possible, through their apprehension, to greatly reduce the rate of that crime type e.g. break and enters.

Forensic intelligence can be further sub-divided based on the level on which it is being used within the law enforcement hierarchy, and the context of its application. Ratcliffe identifies three different levels or categories of forensic intelligence; strategic, operational, and tactical [64], all of which are core parts of intelligence-led policing (ILP). Despite these delineations between the different sub-categories of forensic intelligence, the process of intelligence (i.e. the intelligence cycle) remains the same, with the main difference being the impact the intelligence can have on the criminal environment and overall policing.

Tactical intelligence

Tactical intelligence is the most common level of intelligence used within law enforcement, and has a smaller, more specific focus on achieving case-specific goals [64, 68]. The outcomes of this particular level of intelligence is more on the micro-level, often with individual investigators or small teams producing intelligence in a short time scale to support case specific actions of police or investigators [71]. Such goals could include targeting local criminals, the identification of new leads or making an arrest [64]. This intelligence level often translates

directly into arrests and does not always translate into the bigger picture goals of forensic intelligence, although the intelligence produced at this level could be used for strategic and operational purposes [64]. To relate this more specifically to the identity crime and fraudulent document environment, an example has been included below. Note all locations, websites, names, companies and circumstances are entirely fictitious and have been included for purely illustrative purposes.

Example: There was a noted increase in mail theft and subsequent misuse of personal information reports from individuals that lived on 145th Avenue in Blacktown, NSW, so police informed local banks to pay extra attention, or flag any attempts to open bank accounts or credit cards using an address on this street. A local bank flagged one such attempt to open a bank account and Offender X was arrested. After their arrest, it was found through examining their browser history that Offender X had purchased the stolen personal information, and the counterfeit driver licence that they used at the bank, from an online store "FakeIDsOztralia".

Operational intelligence

This level of intelligence operates more on the meso-level, providing more big picture understanding of longer-term problems such as the operations of criminal networks, spanning multiple crime types and jurisdictions [64, 71]. The outcome of intelligence at this level is to provide investigative teams and decision makers with hypotheses and inferences concerning illegal operations to assist them in planning crime reduction activities. For example, this intelligence could help decision makers in the allocation of resources across a city (i.e. police patrols etc.) or which criminal network or group would be most vulnerable to police action [64,

71, 72]. The main distinction between operational and tactical intelligence is that operational intelligence spans beyond case-specific actions (e.g. making arrests in a specific investigation).

Example continued: Police began investigating the online store "FakeIDsOztralia" and found that the site had thousands of sales logged, all for a range of products, most of which were for fraudulent Australian driver licences. They also found that it was run by an individual that worked under the pseudonym of "Alfred Counterfaker". On the website, high quality images of the counterfeit documents were provided, so police were able to compare the images of the Australian licences to previously intercepted or seized documents of those kinds. Similarities were identified between the Alfred Counterfaker licences, and physical licences that had been seized from the members of an outlawed motorcycle gang (OMCG) that were intercepted as part of a drug operation. From this, police were able to flag the document type, and key characteristics that could help identify other members of that OMCG, and they shared this information with police to assist in the identification of documents that fit within that series, and therefore individuals who may be associated with the OMCG. It also helped illustrate the full activities of Alfred Counterfaker's business.

Strategic intelligence

This level has a stronger focus on studying and understanding the broader criminal environment, how it functions and any current and emerging trends [64, 71, 72]. At this level, the aim is to be future-oriented and proactive and to influence more long-term operational objectives, discussion of policy, resource allocation, and broader strategies [64, 71]. In many cases it is used by senior leadership within the organisation, with the decisions made not just influencing law enforcement agencies but also other government agencies that can help to impact the criminal environment such as health services and city planners [64].

Example continued: Police noticed that almost all the Australian licences that Alfred Counterfaker was selling were Victorian and Western Australian licences, and that Counterfaker was able to replicate the visual security features to a relatively high quality. Police were able to then inform the state governments of the security flaws in their documents, and which security features were not effective in preventing the fraudulent manufacture of the documents. The state governments could then evaluate this and potentially make changes to the document templates to try and reduce the fraudulent manufacture of those document types, thus impacting the criminal environment on a broader scale. The increase in number or complexity of the security features would make it more difficult for the manufacturers to reliably counterfeit the documents.

Despite some resistance to its implementation, the field of forensic intelligence has persisted, with it becoming increasingly common throughout the policing vocabulary [53], appearing in policing mottos, especially within Australia. However, there have been questions over the years regarding how effectively forensic intelligence, and intelligence-led policing have been implemented in practice [73]. While there has been much effort devoted to the expansion of database functionality [74-78] and the formalisation of the intelligence process [1, 79], the implementation of forensic intelligence within policing organisations has been met with some difficulty as well as a range of complications [53, 80]. These complications can be linked to many potential causes, but some of the most notable include the difficulty of forensic science transitioning from what has been its primary role within the judicial system to a more intelligence focussed role [2, 81], the resistance to change often noted within police and security organisations [80] and the lack of unification between forensic intelligence definitions and practical implementation.

Of course, reactive policing will always have its place in law enforcement, as police will need to continue reacting to criminal activities and security incidents [52]. However, to combat more complex and widespread types of crime, such as organised crime, police and forensic scientists need to work together to properly implement intelligence-led policing as a complementary law enforcement model. Furthering these difficulties is the number of trace specific intelligence models that have been the focus of recent research, reinforcing the siloes that forensic intelligence is, by definition, trying to break down. Over the last three decades, forensic intelligence models have been developed and investigated in fields ranging from illicit drug intelligence [7, 82-85], counterfeit medicines and their packaging [86-88], counterfeit luxury goods such as watches [89], deliberate fires [90], and document examination [12, 15, 16, 19, 91, 92].

Quality intelligence is generated through the combination of multiple sources and forms of information to properly understand the criminal environment, thus enabling the design of more effective big picture strategies that can assist in the disruption, prevention, and reduction of that crime type. By splitting efforts across these different trace types, in combination with the division of information sources (often dictated by what organisations own the data e.g. police organisations versus government bodies, and research centres), the ability to generate quality, actionable intelligence is hampered [1]. This was made clear, when Morelato et al. (2014) [1] noted similarities between two intelligence frameworks developed independently in Australia and Europe for monitoring illicit drugs [7] and false identity documents, respectively [1, 14, 93]. Despite the clear differences, both contextually and physically between these trace types, the potential of implementing a transversal intelligence framework that is removed from trace specific constraints was clearly demonstrated [1, 14]. Illustrating that all these trace specific intelligence models, are in fact, unnecessarily dividing the intelligence field, reinforcing siloes.

1.4.1 Forensic intelligence to address complex criminal environments

Forensic intelligence is an effective way to address complex criminal environments, particularly those that are traditionally difficult to access, structured, resilient, and punctuated by prolific offenders and organised crime. One such criminal environment is the market for illicit and prescription drugs. Traditionally, most of the information gathered about the illicit drug market has originated from law enforcement agencies, including but not limited to seizure data and arrest reports. While an important source, these law enforcement statistics are just one facet of information that is often biased towards the focus or goals of that particular organisation [14]. Due to the complexity of the illicit drug criminal environment, seizure data in isolation does not fully encompass the whole of the market. Therefore, much research has been dedicated to understanding the market for illicit drugs from a range of different perspectives, all with the overarching goal of helping reduce, disrupt, and prevent the use, sale, trafficking, and manufacture of illicit drugs [94-98].

Indeed, over the last few decades, an increasing amount of research has been dedicated to understanding how forensic intelligence can assist in improving the understanding of the illicit drug market. This research has ranged from the profiling of illicit drug seizures [82-85, 99-102], examining online marketplaces (i.e. cryptomarkets) to help highlight trends in supply and demand [96, 103-110], examining online trends and discussion forums to help early warning systems for illicit substances [111, 112], to the analysis of wastewater and used injecting paraphernalia to provide insight into what drugs are being used, where they are being used, and how they differed from what the customer thought they were using [113-116]. While this list is by no means exhaustive, this illustrates the many different perspectives from which this complex criminal environment has been viewed. External to this research, there are also a range of government-based research institutions that conduct surveys and produce reports to help illustrate the extent of the illicit drug market such as the National Drug Strategy Household

Survey[3], the Illicit Drug Reporting System (IDRS)[4], the Ecstasy and Related Drugs Reporting System (EDRS)[5], and the Illicit Drug Data Report[6].

All these information sources contribute to better understanding and therefore reducing the supply, demand, and harm associated with the illicit drug market. Whether that be providing information about drug use trends amongst Australian consumers, and where these shipments are likely to be coming from or enabling police and health authorities to help reduce and prevent overdoses by providing warnings of dangerous drug batches due to adulterations or unusually high purity. Specifically, the examination of the online trade for illicit drugs identified a strong domestic market within Australia for illicit substances purchased through the cryptomarkets, suggesting that increased checks of domestic parcels could help to intercept shipments of illicit substances [96, 104, 117]. All these avenues of research and the combination of this information have helped provide insight into a traditionally difficult-to-access criminal environment, creating an ecosystem of more well-informed law enforcement and health agencies that can more effectively make choices and changes to help reduce, prevent, and disrupt the illicit drug criminal environment [37].

Despite the difference in the type of trace and analyses required, there are definite similarities between the criminal environments for illicit drugs, and that for identity crime and document fraud. Both environments have similarities in their structure, being the organised nature, and that they are punctuated by prolific offenders, but also in the breadth of reach of the criminal environment. The illicit drug market is known to have links to and support the activities of organised crime and terrorist groups [118], much like the way that document fraud and identity crime are enablers of other more serious organised crime, including the trafficking of illicit

[3] https://www.aihw.gov.au/about-our-data/our-data-collections/national-drug-strategy-household-survey
[4] https://ndarc.med.unsw.edu.au/project/illicit-drug-reporting-system-idrs
[5] https://ndarc.med.unsw.edu.au/project/ecstasy-and-related-drugs-reporting-system-edrs
[6] https://www.acic.gov.au/publications/illicit-drug-data-report

drugs and other goods [32]. These similarities between the illicit drug and identity crime criminal environments suggests that forensic intelligence could be similarly applied within the area of document examination to assist in the reduction, prevention, and disruption of identity crime and document fraud, coupled with improving the understanding of this ill-defined criminal environment.

1.5 Forensic intelligence through document examination

Despite the successes of using forensic intelligence to help understand the illicit drug market, the adoption of these methods across other criminal environments has been inconsistent. While increasing in the last decade, the concept of using forensic intelligence in the field of document examination has remained generally underexplored in the literature, with practices implemented in operations often developed ad hoc and not formalised. Even within forensic document examination literature and research, the focus has remained predominantly upon authentication and forgery detection, within both physical and digital document examination [119-122]. While authentication and forgery detection are admittedly important areas of document examination, the overemphasis on the development of more technically advanced methods has resulted in some oversight within the field, including an underutilisation of information that can be gained from the simpler, traditional examinations. Realistically, only a small number of fraudulent documents are ever of such a quality that highly sensitive and resource-intensive techniques are required to differentiate them from their legitimate counterparts [15]. This leads to most research having a limited impact on practice [123].

In 2023, Deviterne-Lapeyre et al. conducted a review of all the questioned document literature that had been published between 2019 and 2022. While 1014 papers, textbooks and conference presentations were referenced and examined, only four works (0.4%, three presentations and one article) had a focus on forensic intelligence, with most research focusing on the articulation of forensic opinions [50]. According to this review, between 2019-2022 there were approximately 1,200 conference presentations related to the topic of security documents (only some of which were examined by the authors). Most of these focussed on the authentication of documents and advancements to security features and printing processes [50]. A similar trend was noted in their 2020 review of the literature published between 2016 and 2019, with only four of the 213 papers and presentations examined focusing on forensic intelligence [119]. A

significant disadvantage of this over-emphasis on authentication and detection is that it makes it seem as though the only useful information to be gained from a document is its authentication status i.e. whether it is genuine or fraudulent. However, this is a very limited approach towards documents, as identifying a document to be fraudulent is simply the start of the next challenge, being the extraction of as much information and intelligence as possible from the document.

This imbalance is not anomalous to these review papers. Previous IIFMS (INTERPOL Forensic Science Managers Symposium) reviews of the forensic document examination literature showed a limited but growing mention of the notion of forensic intelligence, particularly since 2010 [124-128]. The lack of intelligence research within document examination is surprising given that ideas related to document intelligence can be traced back to Morton in 1984 [129], who suggested that once a document is identified as fraudulent, two further steps can be undertaken, the first one being to link the document to others based on the comparison of forensic features, the second one being common source attribution. Since this first notion of how document authentication could be extended, there have been numerous additions to this concept. In 1999, Pfefferli et al. [130] suggested that fraudulent documents should be compared to previous seizures in order to, based on forgery techniques, identify series, origin and delivery routes. Friedrich, in 2001 [39] extended this idea further, considering how the different forgery techniques in these documents could assist in the identification of vulnerabilities and the creation of new controls and stronger security features for future documents.

The gradual development of the ideas of document intelligence continued into 2004, with Ng et al. [131] proposing the study of trends in M.O. within the manufacture of documents, and Estabrooks et al. [132] suggesting that documents could be linked based on the quality of their printing. In a report published in 2010 about the use of forensic science to combat and prevent identity-related crime, experts from the United Nations Office on Drugs and Crime (UNODC) suggested that databases could be used to provide law enforcement and forensic scientists with

authentic documents to use as references during the authentication step. Further that this should be used in partnership with collecting information about fraudulent documents to identify linkages between documents, and thus generate intelligence about identity crime [133]. The experts also underlined the lack of awareness related to forensic intelligence amongst policing and forensic actors, as well as a lack of resources to engage in document intelligence [129-131, 133]. Despite this sporadic research that provided suggestions for ways that forensic intelligence could be implemented within document examination, what was still lacking within the field was a systematic forensic intelligence method that could be used to properly understand the pervasive and prolific document fraud criminal environment.

The manufacture and distribution of fraudulent documents occurs on a large scale [42], so much so that document fraud is considered a "cross-cutting criminal threat [that] enables and facilitates most, if not all, other types of serious and organised crime" [32 p.17] . Such documents have been used to facilitate a broad range of criminal activities such as the trafficking of illegal goods, drugs, and firearms as well as in human trafficking, migrant smuggling, large scale fraud, and terrorist activities [16, 25, 32, 42, 43, 47, 51, 92, 134-139]. As put by Kephart in 2015, "to terrorists, travel documents are as important as weapons" [140 p.1]. Beyond the use of fraudulent documents to enable serious crimes, the volume of document fraud is also a challenge, as underlined by the increasing rate of identity crime in Australia, of which document fraud is a key component and enabler [47], especially when considering the use of scans and images of identity documents for identity verification online. This is compounded by the growing rate of demand for and production of fraudulent documents in Europe [38].

The fraudulent document market, which operates on an international level, is punctuated by a small number of organised recidivists who are responsible for a disproportionately large number of the products for sale [15, 141, 142]. These offenders are so prolific that, whether

they be individual forgers or large operations, their production volume has been recorded to range from hundreds of documents, up to millions [15, 141, 142]. The current reactive method, while effective in detecting singular instances of forgery, neglects to consider what should happen to the document after it is identified as fraudulent, and instead, solely takes action against the individual using the document [15, 16].

Much like the illicit drug market, the criminal environments of identity crime and document fraud are complex. International research has proven the efficacy of the profiling of fraudulent identity documents to highlight the structure and organisation of the physical side of the document fraud criminal environment [15-17, 37, 51, 143]. This has culminated in the creation of a web-based program that facilitates the systematic profiling of fraudulent documents, ProFID (standing for Profiling of Fraudulent Identity Documents), which has evolved into the Interstate Database of Fraudulent Identity Documents (BIDIF), implemented in Switzerland and expanding across Europe. However, to obtain the most complete picture of the market, crime traces need to be systematically exploited and combined with alternative information from a range of sources [4], similarly to what has been done within the illicit drug market.

Currently, very little is known about the Australian markets and criminal environments for document fraud and identity crime. There are several approaches that can be used to obtain information about identity crime, such as the profiling of document seizures as well as the analysis of cryptomarket data and crime statistics. Separately, these sources only reflect a small part of the identity crime problem and are usually incomplete as a sole descriptor of the market. Consequently, combining the results of these different information sources, based on traces of different natures would provide supplementary added value, and would provide a far more holistic picture of the overall criminal environment for identity crime and document fraud [1, 14]. Given the borderless nature of identity crime, coupled with the broad and in some cases contradictory definitions and laws used to try and prosecute identity crime, a more holistic

approach is required to improve the understanding of this criminal environment. Adopting this approach will also provide a realistic insight into document fraud within Australia, how it is structured, and what may need to be changed to more effectively disrupt this repetitive and pervasive criminal problem.

1.6 Aims of this thesis

This research will use the profiling of Australian fraudulent identity documents in combination with online cryptomarket analyses to provide a more holistic view of the criminal environments of document fraud and identity crime in Australia. As illustrated both by the research conducted in the illicit drug criminal environment, and explained in the previous section, a multi-source approach is integral to properly understanding a criminal environment, so that is the approach followed here. This criminal environment is examined from two different perspectives, focussing on the physical market (as indicated through the examination of the physical traces of the market, i.e. seized documents), and then the digital market for fraudulent documents and personal information (i.e. that facilitated through the internet). This is followed by an examination of how these seemingly dichotomous information sources can be used together to provide a holistic understanding of document fraud and thus identity crime within Australia, and how this can be used to assist in intelligence-led policing. The overarching aim of each chapter has been included below, but the specific objectives of each section have been included in the relevant chapter.

Chapter 2 focuses on examining the physical side of the market, through the examination of fraudulent Australian licences that have been intercepted by police and security organisations. The overall aim of this section is to illustrate how fraudulent identity documents as a type of trace have been underutilised within Australia, and how their systematic profiling and comparisons can provide intelligence to gain a better understanding of the fraudulent identity document climate within Australia.

Chapter 3 focuses on the digital (online) market for fraudulent identity documents and personal information. This chapter aims to determine, through the analysis of two anonymous

online marketplaces (i.e. cryptomarkets), if the online market for fraudulent documents and personal information is organised, and punctuated by prolific offenders, both on the larger international scale, and from a more Australian focused perspective. Furthermore, the variety of information that can be gathered from this marketplace, as well as how this can assist intelligence-led policing is examined.

Chapter 4 examines the potential of using the seemingly separate information sources covered in Chapters 2 and 3 in combination to provide greater understanding of the complex criminal environment for identity crime and document fraud. These two portions of the illicit market are compared to illustrate the importance of using a multi-source approach when examining the illicit marketplace. Furthermore, it is proposed that these two sources of information can be combined and used as part of a multi-source, holistic intelligence framework, integrating information gathered from a range of government organisations to better understand the criminal environment of identity crime and document fraud.

The Forensic Profiling of Fraudulent Identity Documents

2 The forensic profiling of fraudulent identity documents

2.1 Introduction

While suggestions of the potential benefits of expanding document examination into a quasi-intelligence space traces back to Morton in 1984 [129], it wasn't until 2012 that Baechler et al. published a systematic forensic intelligence model for the profiling of fraudulent identity documents [15]. This method addressed the prolific nature of the fraudulent identity document criminal environment and suggested a way that the environment could be characterised and then tackled in a more proactive manner. Since then, this method has been expanded to consider a broad range of information that can be extracted from these documents, and a systematic method for profiling the visual and digital image processing features of fraudulent identity documents has been implemented in Europe and is expanding internationally [13, 15, 17, 143]. Despite this success, no research has been dedicated to the investigation of how a systematic intelligence model could benefit Australian intelligence-led policing, and how it might assist in understanding the criminal environment for document fraud in Australia. In this chapter, the focus will be on understanding the physical side of the fraudulent document market in Australia through the forensic profiling and comparison of fraudulent identity documents seized by police. The organisation and structure of the market will be examined and compared to that in Europe to evaluate if the systematic intelligence method implemented internationally could be successfully used in Australia. The theory behind the profiling method is first introduced, and then the use of the profiling method on Australian documents will be tested. The outcomes of this method, along with the feasibility of implementing it within Australian policing and security organisations is then discussed.

2.1.1 Forensic profiling as a tool for forensic intelligence

In forensic intelligence the term ‘profiling’ refers to the selection and extrapolation of information from a trace to generate a set of features (i.e. profile) that are characteristic or representative of that trace, similar to what is done in DNA profiling. This can then be used as a ‘model’ of that trace [15, 144]. The ‘profile’ can be used as is, or converted into a numerical form, to easily compare traces between sets (or instances of criminality) to determine linkages. In 2012, Baechler et al. suggested the utility of using profiling within the realm of document examination, focusing on the visual profiling of fraudulent identity documents to try and identify those that were likely to have been produced using the same methods, and therefore likely to originate from the same source (i.e. forger) [15, 144]. This work aimed to expand the potential of document examination processes, moving beyond simple identification and authentication of documents, to instead consider the value that can be gained by examining them within a systematic and methodical forensic intelligence process [15, 16, 144].

At the core of the profiling method for fraudulent documents is the examination of features, being the characteristics imparted on the documents by the forger, during their manufacturing process. The major premise behind this method is that a source, whether that be an individual or an organisation, will produce documents using the same M.O. [15, 16, 144]. This M.O. will be based on what the source knows, the techniques available to them, what the source has, i.e. the materials and equipment, and also what their physical characteristics are, such as fingerprints or DNA [15, 144], as illustrated in Figure 2-1.

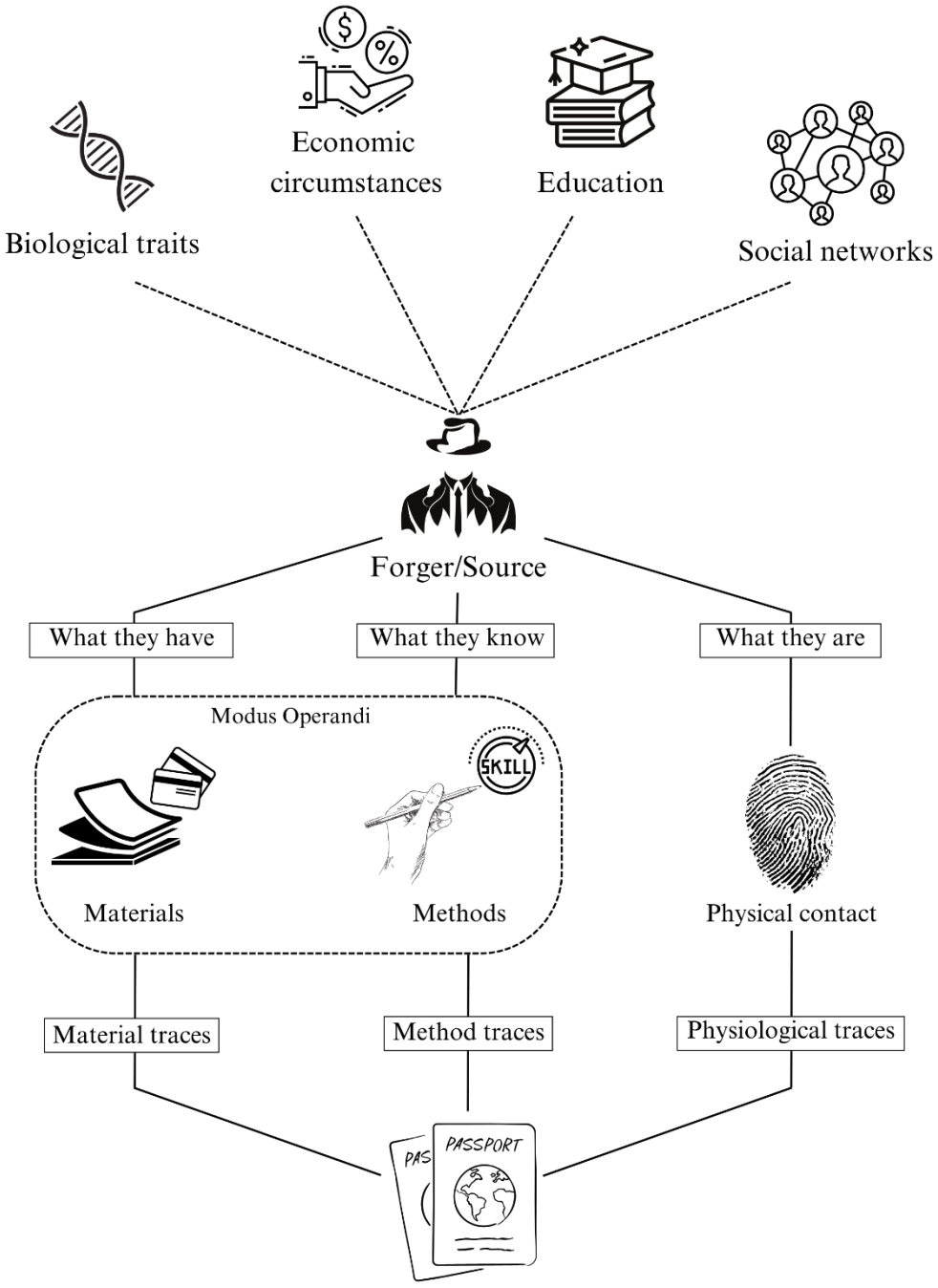


Figure 2-1: The major and minor premises of the profiling method suggested by Baechler et al. in 2012 [15]. This illustrates that the biological traits, economic circumstances, social networks and education will influence the choices made by the forger in relation to the M.O. used to create documents. This in turn impacts the traces that can be observed on the fraudulent identity documents. Figure adapted from [1, 13, 14, 144]

While this explains the premise behind the ability to group documents together, the minor premise of this method is that different sources will produce fraudulent documents using different methods, materials and M.O. based on their economic situation and education (Figure 2-1). Another potentially influential factor is the forger's social network including, but not limited to, their contacts and mentors. Depending on who they are in contact with, and who their suppliers and teachers are etc., this may impact the techniques and materials that they use, and perhaps even the types of documents they choose to manufacture. All of these potential variations will result in different material and method based traces being imparted on the documents, with the manufacturers biological traits (e.g. fingermarks and DNA) also dictating the physiological traces they may leave behind due to physical contact with the document [15]. Therefore, the similarities or differences between a document profile can be used to infer that the documents were manufactured using the same or different M.O. and therefore whether they have originated from the same or different sources [15] as illustrated in Figure 2-2.

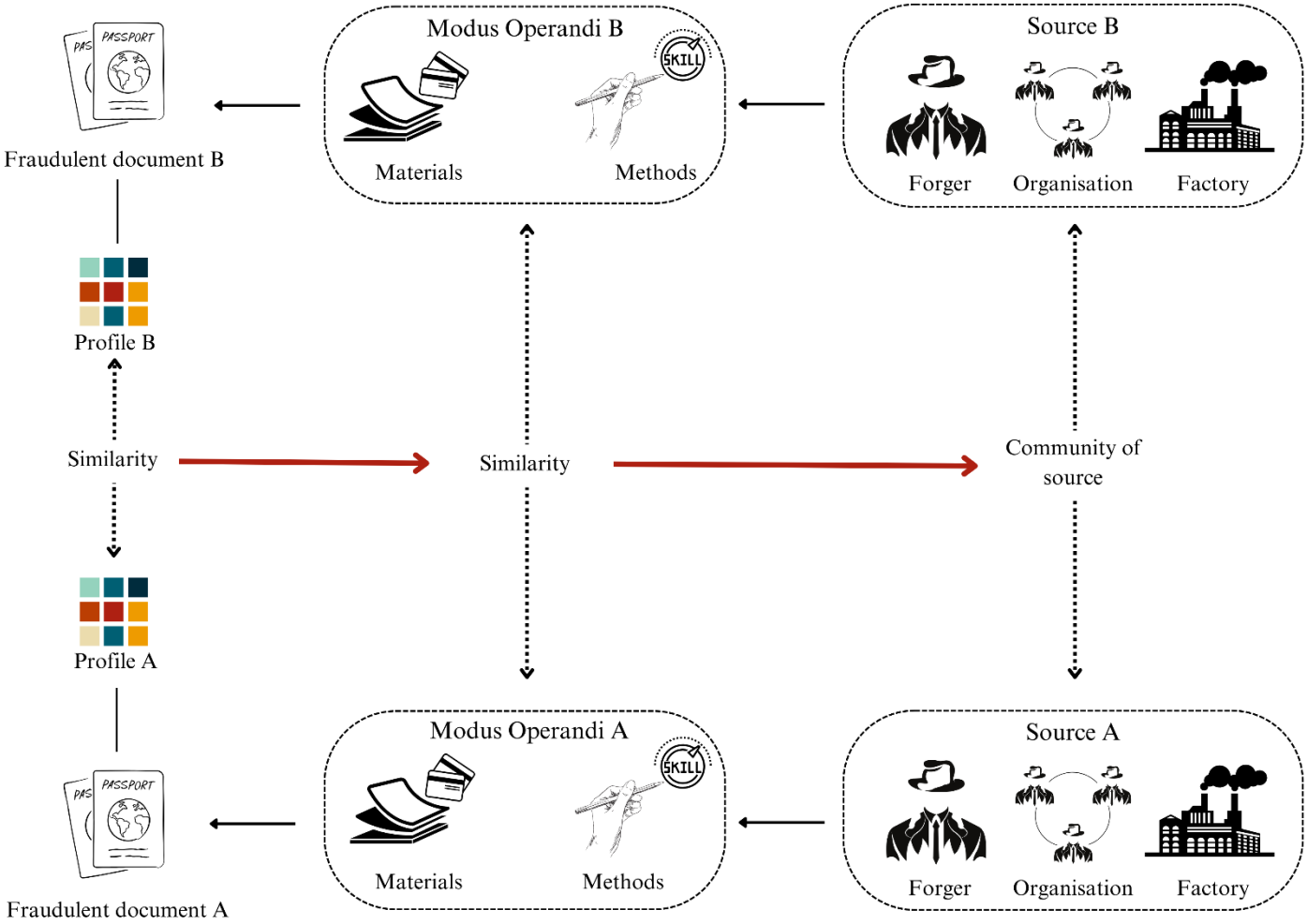


Figure 2-2: The profiling method illustrating how the different sources use different M.O.'s that therefore impart different traces onto the documents. By comparing these traces using profiling, the similarity of two profiles can indicate a similarity between the M.O.'s used to create the document. This can then indicate a similarity or community of source that produced those documents, whether the source be a forger, an organisation of forgers or a factory doing mass production. Figure adapted from Baechler et al. 2012 [15].

Naturally, one may question whether a forger's M.O. will evolve over time resulting in a change in the traces that they leave on their products. While this is always a possibility, given the repetitive nature of fraudulent document manufacture, and in accordance with rational choice and routine activities theories described in criminology [145, 146], these traits and the M.O. are considered constant enough that it is possible to draw links between documents manufactured by the same source [15, 16, 144]. Rational choice theory states that a criminal

will use a logical thought process to analyse and weigh the potential costs and benefits of committing a crime with their decision to offend based on whether the costs of the act are outweighed by the potential benefit [145]. It is therefore considered unlikely that a forger will make drastic changes, replace functioning equipment, or abandon tried and true methods or knowledge, as the cost of this to their business would undoubtedly outweigh the benefits [15, 16, 144]. An exception to this, however, may be if changes are made to accommodate advancements in document security (i.e. the security features used in legitimate documents) and manufacturing tools. Even in these cases, while an individual characteristic, or portion of the method may change, other aspects of the M.O. are likely to remain the same, so by using a variety of features within the profile, it will still be possible to link documents together, and to perhaps even illustrate the evolution of the M.O. over time [13, 51].

Historically, the adaptation of the M.O. of forgers, sometimes described as a kind of *crime displacement*[7] [147-149], has often occurred with changes and developments to document security and policing methods [27, 28, 120]. One such example of this was the change in M.O. exhibited by forgers after the change of the Swiss identity card from a paper-based document to a plastic credit card style [13, 51]. In the original paper-based document, there was a watermark that was difficult to convincingly replicate, so rather than attempting to counterfeit it, forgers would instead alter legitimate versions. After the transition to the laser-engraved credit card style model, forgers switched their M.O. to instead start counterfeiting the document, as the credit card style was too hard to forge [13, 51].

Further illustrating the consistency in M.O. used by forgers is the rather static nature of the quality of fraudulent identity documents. Baechler and Margot (2016) identified that the quality of fraudulent identity documents remained consistently low across periods of up to thirteen

[7] The relocation of crime from one place, time, target, M.O. etc. to another [147, 148].

years [13]. It is hypothesised that as the demand for fraudulent identity documents is often smaller on a per client basis, i.e. each client will usually only use one fake identity at a time, there is not as much of a need to be constantly changing and updating their methods [13, 51]. However, it must be noted that only those documents that are of low enough quality to be detected as fraudulent are seized by police, undoubtedly resulting in some level of bias, as those that are of the highest quality are less likely to be intercepted or seized.

The profiling of fraudulent documents can provide intelligence beyond just identifying those documents most likely to have been produced by the same source, with the method contributing to the three different levels of the intelligence process as defined by Ribaux et al. in 2003 [150], reminiscent of the general levels of forensic intelligence, strategic, operational and tactical [64] discussed in Section 1.4. This three-level architecture is defined as:

1. Surface or strategic level
2. M.O. level (operational)
3. Series level (tactical)

Surface or strategic level

The surface or strategic level of the forensic intelligence process, focuses on the most general considerations, aiming to provide information on bigger picture issues such as the evolution of the criminal environment over time to provide an understanding of the overall crime problem [15, 150]. By examining the most general features of the documents, such as the document type, fraud type, and issuing country, this can provide indications as to the state of the criminal environment over time, and trends in the manufacture and distribution of these documents, internationally (if appropriate information sharing is in use) [15].

M.O. level

The focus of this level is to distinguish the different M.O. that have been used to provide a clear understanding of the criminal environment and to differentiate between anecdotal cases of crime and those that are being carried out by organised crime networks [150, 151]. This is done by profiling the documents based on their features so that they can be compared and organised into different series that reflect the M.O. used to create them [15]. This can assist in connecting cases and highlighting the structure of the criminal environment.

Series level

The final level, and the one that requires the most detailed examination, focuses on individual series and cases to identify whether proposed links exist and to fully illustrate the extent of the criminal activities of a particular source. For example, if a large shipment of documents is intercepted through the post coming into a country, and the sender is then arrested, all the documents that were intercepted could be compared to those that were previously collected and examined to provide an indication of the full extent of that sources' criminal activities.

The basic premise of this profiling method is transversal, meaning that it can be applied to a range of different trace types, depending on the goals of the analysis and what is accessible to the examiner. In the realm of document intelligence research, three different types of features have been targeted, or profiled, to try and help address the ever-increasing criminal environment of identity document fraud: visual, digital, and chemical features (Figure 2-3). Each of these different types of features and their profiling processes are explained further in the following sections.

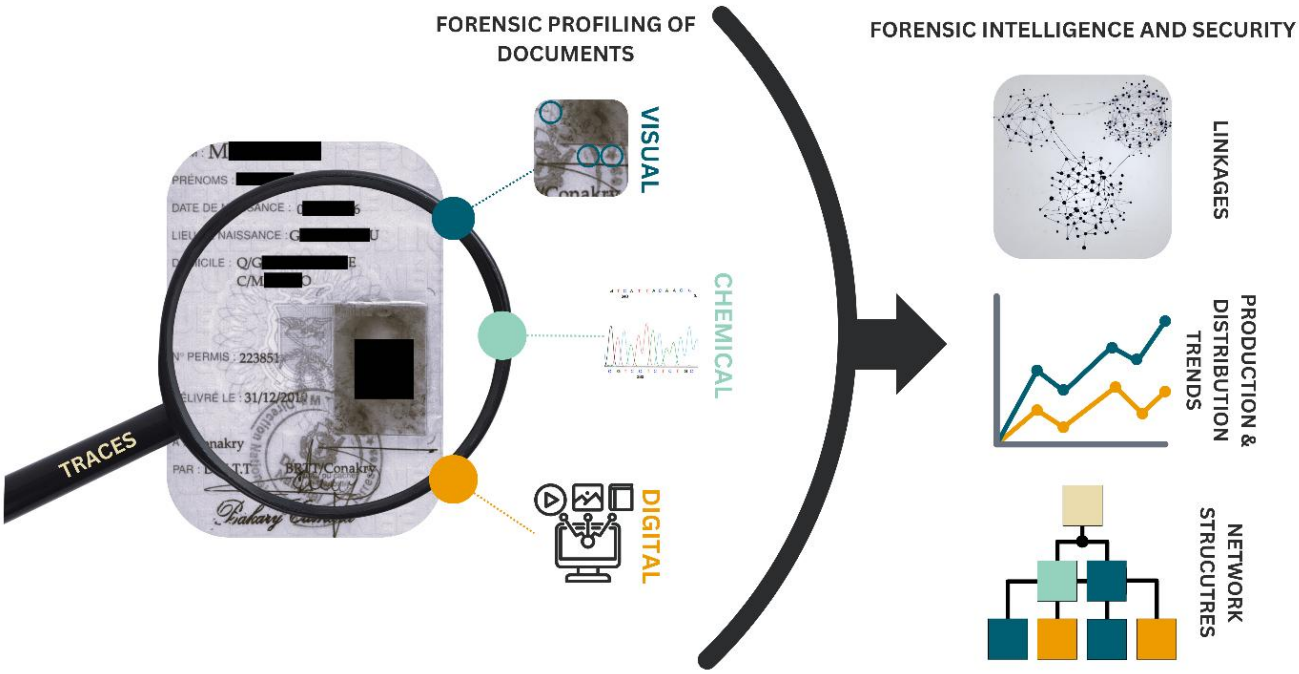


Figure 2-3: From a fraudulent identity document one can extract visual, chemical, and digital characteristics that can be used in a forensic profiling method to gain insight into the criminal environment. This can take the form of identifying linkages between sources, trends in production and distribution and identifying the structures of criminal networks.

2.1.2 Forensic profiling of visual features

2.1.2.1 Visual features of fraudulent identity documents

Identity documents and security features are, by their very nature, visual objects, and their authentication relies largely on the presence, quality, style, and special properties (i.e. ultra-violet luminescence) of visual features. Therefore, it was a logical first step to use these visual features to create profiles to enable the systematic comparison of fraudulent identity and security documents.

While an exhaustive list of the features that have been used within the forensic profiling method cannot be provided (as this is sensitive and in most cases protected information), some of the features that are targeted include things such as [15]:

- Serial and document numbers
- Fonts
- Printing methods (inkjet, laser etc.)
- Replication of security features such as watermarks, stamps, ultra-violet (UV) features, and microprinting
- Mistakes or errors in the template

All these features are intrinsically linked to the method of manufacture of the documents and therefore reflect the choices of the forger at different points in the manufacturing process, as illustrated in Figure 2-1 and Figure 2-2. They can therefore be used within the profiling method to help identify those documents that have been made by the same source [15].

Visual characteristics were the initial target of this method as they are easily accessible, efficient, and cost-effective to profile. The fact that they are easily discernible using basic tools such as the naked eye, optical microscopy, and UV light, means they are not only cost-effective to extract but can be extracted by anyone regardless of their training or familiarity with counterfeit documents. The features can also be easily extracted making them efficient targets for the profiling method, with previous research illustrating that a single document could be profiled in under 10 minutes, depending on the level of depth required in the analysis per the intelligence level being addressed (Section 2.1.1) [13, 15, 17].

2.1.2.2 Extraction and comparison of visual features

After a document is seized, it is visually examined under white light and UV light and then photographed and scanned. To create the profiles of the documents (Figure 2-4), the features of interest are identified, extracted, and then codified, often converting the features into numerical values, as illustrated in Table 2.1. These numerical values are then compiled to create the profile of the document. As an example, the profile of the document from Table 2.1 would be (1,3,5,26507084,1). This profile would then be stored and structured within a memory where the profile is compared systematically to all other documents of the same type using optimised comparison metrics[8] [152].

Table 2.1: Example profile of a document, illustrating the conversion from features to the numerical profile. Please note that is an oversimplified example of a profile.

Feature	Shortened profile	Numerical
Coat of arms style 1	COA1	1
Microprinting style 3	MP3	3
OVD style 5	OVD5	5
Serial/ID number	26507084	26507084
Inkjet printing	1	1

These metrics compare the profiles of the documents to determine whether they are the same. The result of this process is a similarity score (ranging from 0 to 100) which indicates the level of affinity between the profiles. Depending on the threshold set by the operator, these similarity scores can be interpreted as being either the presence or absence of a link. If a link is present,

[8] Comparison metrics, sometimes referred to as distance metrics were used in Baechler et al.'s [13, 15, 16] research to calculate the numerical distance, or dissimilarity between data points within a profile [152].

then the documents could have been produced by the same manufacturing method or M.O., and they can therefore be considered as likely sharing a common source [13, 15, 16].

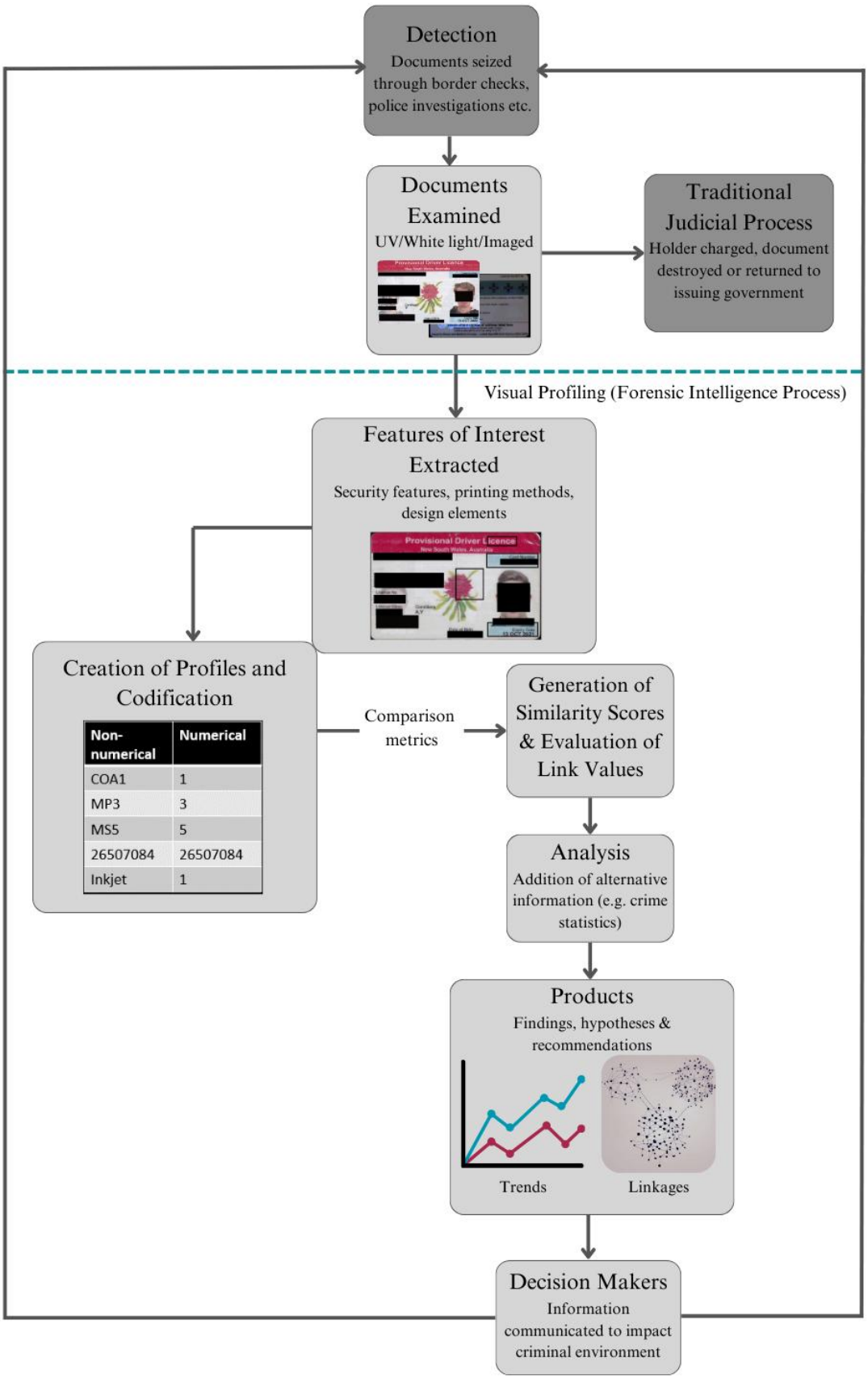


Figure 2-4: The forensic intelligence process for fraudulent identity documents. Adapted from Morelato et al. 2014 [1].

The analysis of the documents profiles of course goes beyond just the identification of linked documents and series, and with treatment of external information, trends in manufacture, distribution and use of the documents can be identified. When this information is provided to decision makers this can assist in providing further understanding about the criminal environment, contributing to efforts to disrupt, reduce, and prevent the actions of prolific offenders.

2.1.2.3 Efficacy of the method

This method has thus far been used in a range of studies, and its efficacy has been proven across not only different document types (such as passports and identity cards) but also different fraud types (e.g. stolen blanks, counterfeits, and forgeries) and from different issuing countries. Two studies were conducted, one in 2012 in which they examined 393 fraudulent identity documents from a pre-existing Swiss authentication-focused database, known as FRAUDE [15], and the second in 2016 in which 363 fraudulent identity documents were analysed [13]. Across both studies, the documents varied in document type, forgery type, and issuing countries. Despite these differences, the profiling method revealed over 50% of the documents examined were linked to at least one other document [13, 15], as shown in Table 2.2.

Table 2.2: Results from the visual examination and profiling of 393 fraudulent documents that were seized by nine different Swiss police forces and other foreign authorities [15] and 363 documents that were seized across a variety of jurisdictions in France and Switzerland between 2000 and 2012 [13]

Study	Fraud type	Country of issue	Document type	Number examined	% linked
2012	**Counterfeit**	Portugal	Identity card	170	68%
	Stolen blank	France	Passport	59	58%
	Forged	Bulgaria	Driver licence	32	40%
	Counterfeit	Iraq	Driver licence	132	31%
2016	**Counterfeit**	France	Identity card	129	69%
	Counterfeit	Portugal	Identity card	170	67%
	Stolen blank	France	Passport	64	63%

The method proved to be both efficient and effective at identifying links, with the number of links detected using the intelligence method doubling what had previously been identified during the investigations [15]. Furthermore, all but one of the original links identified through traditional investigative means were identified through the forensic intelligence process, with the links crossing not only jurisdictions but also borders, illustrating the efficacy of this method in reducing linkage blindness [153]. While clearly effective at linking documents together, the ability of the method to group documents that were known to originate from a common source was evaluated in a 2013 validation study [16]. The researchers were able to illustrate a clear distinction between intra- and inter-source variations, with false negative and false positive error rates consistently remaining below 0.75%, well within the acceptable uncertainty range of forensic intelligence [16].

From this work, it was clear that not only were fraudulent identity and travel documents useful tools for understanding the structure of the criminal environment, but that their visual

characteristics were ideal for the construction of the profiles. Their comparison was successful in linking documents together that had been produced by the same source, while also differentiating those that had been made by different sources [13, 15].

2.1.3 Forensic profiling based on image processing techniques

Where the original work by Baechler et al. focussed on the comparison of manually extracted visual characteristics, there has been increasingly more research dedicated to investigating the application of the profiling method in a more digital space. Given that much of forensic intelligence aims to produce actionable intelligence as efficiently as possible, it was questioned whether the profiling method could be made more efficient with the addition of an automated triaging step, while also adding another aspect of comparison. Not replacing the manual human-driven method, but rather complementing it, attempting to further the development of a human-machine coupling approach.

In these methods, researchers began investigating the use of a combination of image processing filters and data processing techniques, to assist the manual profiling method and to introduce a degree of automation into the characteristic extraction [19]. This method was further developed by Auberson et al. who introduced the use of a computer vision-based method into the previously established intelligence framework [92]. Inspired by methods used to manage digital images of Ecstasy tablets [154], Auberson et al. postulated that, in the same way that similarities in visual characteristics of the documents could be used to indicate a community of source, so too could similarities in image processing methods such as colour, hue and texture.

2.1.3.1 Regions of interest

Where the visual profiling method focuses on visual features of interest such as the type of font, printing, and replication of security features, the profiling method based on image processing techniques focuses more on the pixel-by-pixel comparison of regions of interest (ROI's). Generally, these regions of interest can be selected anywhere on the document, avoiding areas that contain personal information likely to change between holders of the document. Areas that perform the best are those that have a high degree of variation in the colour and shades, and areas that are likely to include traces left from the manufacturing process such as printing, colours, and areas with design elements such as logos [92]. After the regions of interest are selected, the image is automatically cropped, and then the regions of interest are imported onto the web server, where the filtering and comparison process begins.

2.1.3.2 The method and its performance

Once the images of the ROIs are imported into the web server, the individual images are processed using ten common image processing tools: red/green/blue; grey levels; hue/saturation/brightness; contrast, texture and edge. Profiles were derived from the histograms from each image and were subsequently compared using metrics (Euclidean, Manhattan and Canberra distances). These metrics produced a similarity score which indicated the affinity between profiles as illustrated in Figure 2-5. The method was applied to a data set of 32 counterfeit Portuguese passports and 26 counterfeit Italian driving licences, and much like the original profiling method, showed very promising results. The counterfeit Italian driving licences were classified with an exceptionally high accuracy[9] of 92.4%, with the counterfeit Portuguese passports close behind with an accuracy of 90.3% [92]. While the accuracy rates of the validation set were somewhat lower with an accuracy of 71.4% and 88.2% respectively,

[9] In the work by Auberson et al. the accuracy of the method was evaluated based on the correct grouping of documents of known common origin within the same group, or branch of the dendrogram, while also separating documents of different origins into different regions of the dendrogram [92].

the misclassifications encountered were often due to differences in the physical appearance of the licences, either due to wear and tear, fading, or inconsistent ink supply during the original printing of the document [92]. Used in conjunction with the original profiling method, it provided a rapid triaging system to help explore large data sets and indicate potential classes or relationships that warrant further examination [92].

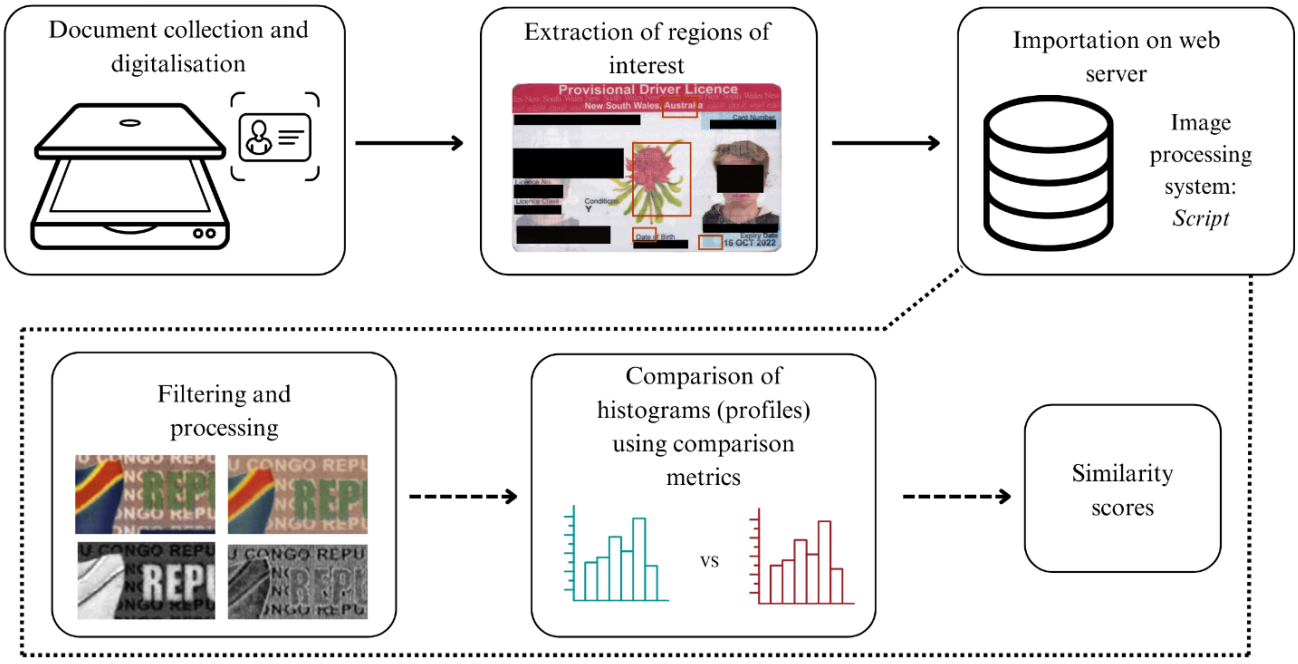


Figure 2-5: Flow diagram illustrating the method for profiling using image processing techniques. Adapted from Auberson et al. 2016 [92]

There have been a few other papers that have created and tested different versions of an automated document comparison method. Work by Vieira et al in 2016 and 2017 looked at the use of digital image processing techniques coupled with algorithms such as Harris Corner Detection[10] and Scale-Invariant Feature Transform (SIFT)[11] to assist in identifying documents

[10] A mathematical approach used to detect and extract the corners and edges within an image [155].
[11] The SIFT algorithm was developed and used within Vieira et al.'s research [156, 157] to ensure that the zoom or rotation of the image would not impact the calculation or extraction of the corners and edges [158].

that were created using similar M.O. [155-158]. More recently, Ojeda-Aciego et al. examined the potential of using Formal Concept Analysis (FCA)[12] to assist in the detection and comparison of forgeries to help in obtaining details about the forgers activities [159]. While Vieira et al.'s methods shared more similarities in structure to the work conducted by Auberson et al., the work using FCA had a simpler approach, creating the documents profile based solely on whether security features had been successfully replicated. This led to a binary sequence of Boolean values that were then compared between documents [159]. Both methods proved useful as potential triaging tools for large document sets, however Ojeda-Aciego's method, while quicker, may prove to be less useful in identifying series and their evolution in M.O. over time. By focussing solely on whether a security feature was replicated, rather than how it was replicated, the value of the links that can be identified between documents would be decreased from an intelligence perspective.

In a slightly different vein, Girelli et al. shifted focus from creating an automated comparison method, to instead investigating how the use of a common database could assist in generating intelligence to understand the market for Brazilian identity documents [160, 161]. Through their use of the Brazilian Federal Police Automated Fingerprint Identification System (AFIS) they identified that of the 100 images of fingerprints that they had collected from the internet, 31% of them had been used in forged Brazilian ID documents [160]. Furthermore, some of the identified criminal cases involved multiple fraudulent identity documents, all with the same fingerprint image used, clearly illustrating the potential of visually profiling the fingerprints to assist in the identification of links between document sources [160]. While the utility of this comparison process is limited to documents that have fingerprints as part of their template, the potential of comparing traces recovered on the documents to already established databases is

[12] FCA is a data analysis technique that creates concept lattices or frameworks to illustrate the relationships between a collection of objects and their attributes or properties [159].

an excellent example of how these already established facilities can be used to assist in the pursuit of forensic intelligence, minimising costs, and maximising the production of intelligence.

The research discussed above assisted in expanding the profiling method for fraudulent identity documents, illustrating ways that a more automated method could be used as an effective triaging system, while also highlighting other potential features of interest, and how they could be compared to pre-existing databases to extend the potential intelligence that can be gathered from these comparisons.

2.1.4 Forensic profiling of chemical features

The use of chemical analyses within forensic document examination is widespread, however, the use of these chemical analyses within forensic profiling, i.e. creating a profile for the document based off the result of chemical analyses, and then comparing those profiles between documents has been less explored within the literature. With the use of polymers in documents increasing, Mireault et al. in 2017, decided to investigate the potential of using chemical profiling on polymer substrates as an addition to the current profiling method [18]. Due to the highly variable nature of the composition of polymers, the researchers believed that they would be able to differentiate the chemical profiles of polymer cards from different sources and manufacturers using high-performance liquid chromatography – quadrupole time of flight mass spectrometry (HPLC-QToF). In their case study, they examined 60 genuine and false driving licences from Nigeria and Bangladesh, some of which were already identified to be linked due to their visual profiling. They found after their chemical profiling that the forgers were using a different plastic substrate from the genuine documents, and they were able to connect the visually linked documents based on their chemical profiles, indicating that they were produced using the same M.O. and that the same substrate was used in their manufacture [18]. While this

method is limited, in that it can only indicate whether cards were made by the same manufacturer, it does have the benefits of enabling some profiling of blank polymer cards and substrates and would enable comparison between documents of different types e.g., passports and driver licences, that cannot be compared based on visual features.

However, some of the benefits of the visual profiling method are its accessibility i.e., the targeting of easy to access visual features that require no specialised training nor specific equipment, its efficiency, and that the features can be extracted without damaging the document. The incorporation of chemical profiling, while providing an interesting new characteristic to compare, would reduce the overall accessibility of the profiling method as it would require specialised equipment and training, and in most cases would involve the destruction of the document.

2.1.5 Forensic profiling in practice

The potential of using forensic profiling (visual and image based) for the examination of fraudulent identity documents (FIDs) has been recognised since Baechler's initial work, so much so that a systematic method for the profiling of fraudulent identity documents was created and has been used in an operational context initially in Switzerland in 2017, then internationally. This system known as ProFID (standing for Profiling Fraudulent Identity Documents) was developed by the School of Criminal Justice of the University of Lausanne in collaboration with forensic document experts from Swiss law enforcement agencies. Using visual features, it facilitates the profiling and comparison of fraudulent identity documents to assist in identifying those likely to have been produced by the same source [162]. Documents are examined, with their technical characteristics being described, before being scanned and uploaded into ProFID. Once within the secure web platform, the profiling of the document is carried out and a comparison is done between the new document, and all documents of the

same type within the system [162]. Between 2017 and 2020, 2,000 documents were integrated into the ProFID system, which revealed 51% of those documents belonged to one of 150 identified series [51]. Since then, over 11,000 documents have been integrated from 14 different countries across Europe and 25% of them have been identified as linked [163]. In addition to the facilitation of the manual profiling and comparison, automatic image comparison methods based on computer vision have also been integrated within ProFID to assist in the identification of series, based off the work conducted by Talbot-Wright et al. [19] and Auberson et al. [92] as described in Section 2.1.3.

Out of the work on ProFID grew the Interstate Database of Fraudulent Identity Documents (BIDIF) that has been implemented in Switzerland. Given the often-subjective nature of visual profiling, and the implementation of this tool across a range of Swiss cantons and policing agencies, Moulin et al. [17] investigated how an efficient and more standardised method could be applied to the profiling workflow of BIDIF and ProFID. To move the method forward, they took inspiration from the analysis, comparison, and evaluation (ACE) method that was first introduced into document examination by Huber in 1972 [164]. They defined the steps of the method, from the documents initial inception into ProFID, through its analysis and profiling of its features, its comparison to other documents within the database and finally its evaluation of its series status. The use of the method, along with its clear definitions and delineations between classes of characteristics, enabled the professional examiners to more clearly explain how they had identified the links and series of documents [17].

The document profiling approach has also proved to be effective at a cross-border level. Documents seized across France and Switzerland (434 and 2,143 respectively) were examined to identify the potential of cross-border comparisons of fraudulent identity documents [143]. Using the method previously published by Lugon Moulin et al. [17], it was found that 19% of the documents examined from France and Switzerland were linked to documents from the other

country, identifying 33 Franco-Swiss series that totalled 484 documents [143]. These transnational links extended series that were previously identified on a national level, illustrating the contribution of forensic intelligence to investigations and cross-jurisdictional cooperation [143]. This research resulted in the founding of the Internal Security Fund (ISF) ProFID project[13] funded by the Internal Security Fund - Police of the European Commission [143]. Forensic and law enforcement agencies from 16 European countries are involved in this project with the support of several international organisations, namely Frontex, Europol, CEPOL and Interpol. In this framework, more than 400 document examiners were trained across Europe to use the ProFID system and approximately 11,000 fraudulent documents were profiled (25% of which were linked to at least one other document), and around 500 series associated to potential organised crime groups were identified [143, 163]. This underlines the key contribution forensic intelligence can bring at the international level [162].

In an operational sense, the method has shown great success at impacting the criminal environment of document fraud and organised crime. In 2020, this forensic profiling and comparison method was vital in the detection of a document fraud network that had been operating across France, Germany and Switzerland, as well as other EU countries [37, 165]. This criminal group had been producing false documents in Athens that were subsequently shipped throughout Europe to irregular migrants from North Africa. The profiling method was crucial not only to the detection of this criminal network, but also in building the case against the arrested leader of the syndicate [37, 165].

2.1.6 Gaps in the current implementation of document intelligence

It is clear from the research that has been conducted that the visual and digital profiling methods are efficient and effective at identifying links between documents, proving that they are

[13] Project ISFP-2020-AGPOLCOP n°101036247

powerful tools in illustrating the structure of the criminal environment. The transversal nature of the profiling method has also been established through its success on multiple different document types and in the breadth of different countries that have so far implemented the ProFID/BIDIF systems across Europe (14 countries) [163]. However, at this stage, most research has been concentrated in Europe, with only a recent exploration occurring in Canada, leaving Australia and the Oceanic region largely unexplored. This lack of understanding of the Australian fraudulent document market is surprising and likely hampering the overall understanding of the fraudulent document criminal environment, especially considering the presence of Australian documents on the dark web [47, 51], coupled with the high identity crime rate in Australia [29-31, 44, 46, 47] and the documented presence of Australian based organised crime groups and outlawed motorcycle gangs (OMCGs) [139, 166-168].

This is especially relevant when considering the cross-border nature of identity document fraud and identity crime in general, which operates across a broad, international canvas. This gap in the fraudulent document criminal environment, from both a research and policing perspective has resulted in the potential of fraudulent identity documents as traces being underexplored and underappreciated in Australia. To properly illuminate the criminal environment in Australia and illustrate how these traces could be better exploited, the criminal environment of document fraud needs to be more closely examined, and the potential of utilising the systematic profiling of fraudulent documents in Australia, must be explored. This work is a crucial first step towards implementing a systematic forensic intelligence method for the examination and comparison of fraudulent identity documents in Australia (such as the internationally implemented ProFID/BIDIF system).

2.2 Aims and objectives

This chapter focuses on the examination of the physical side of the fraudulent document market within Australia through the analysis of fraudulent documents seized by Australian law enforcement organisations. By visually examining, profiling, and comparing these often-underutilised fraudulent documents, this work provides valuable insight into the criminal environment for document fraud and identity crime within Australia. In accordance with Kirk (1963) [169], instead of focussing on developing a new, context specific method for profiling Australian documents, this work focusses on answering a more fundamental question of whether fraudulent document profiling can provide insight into the Australian criminal environment for document fraud and identity crime. Consequently, in this chapter, the use of the internationally established profiling method (the BIDIF/ProFID system) within the Australian context is investigated. The following objectives are addressed in this chapter:

1. The investigation of how visual profiling techniques and methods can be applied to Australian fraudulent documents.
2. The analysis of the current fraudulent document climate and the determination of whether there is an element of organisation behind the creation and use of fraudulent identity documents.
3. The evaluation of whether a systematic forensic intelligence model for the profiling and comparison of fraudulent documents (such as the BIDIF system) could be implemented in Australia and how this could assist in intelligence-led policing.

2.3 Materials and Methods

2.3.1 Document information

The data used in this research comes from the New South Wales Police Force (NSWPF) and two other Australian policing and security organisations that will remain anonymous. The document types that were examined in this research were collected from police stations and security organisations based in New South Wales and Victoria and included plastic 'credit card' style New South Wales (NSW), Western Australian (WA) and Victorian (VIC) driver licences, along with NSW photo cards. Four international driver licences were also examined, along with four pseudo documents. The full breakdown of the documents is provided in Table 2.3 below, with examples for each of the Australian documents provided in Appendix Table A. 3.

Table 2.3: The breakdown of all documents included in the data set including the organisation that provided them, the type of fraud, type of document, and issuing country/state. Note: Licence (P) refers to restricted, provisional licences, while Licence (F) refers to unrestricted, full licences. The international licences have no letter designation as this was either not present, or unclear.

Organisation	Type of fraud	Issuing country	State	Document type	Number
Organisation 1 (n=56)	Counterfeit	Australia	NSW	Licence (P)	4
				Licence (F)	31
			WA	Licence (P)	1
				Licence (F)	5
			VIC	Licence (P)	15
Organisation 2 (NSWPF) (n=73)	Counterfeit	Australia	NSW	Licence (P)	26
				Licence (F)	7
			WA	Licence (P)	4
				Licence (F)	9
			VIC	Licence (P)	1
		United Kingdom	-	Licence	2
		New Zealand	-	Licence	1
		Papua New Guinea	-	Licence	1
	Forged	Australia	NSW	Photo card	18
	Pseudo	Australia	NSW	Age proof card	2
				Student ID	2
Organisation 3 (n=54)	Counterfeit	Australia	VIC	Licence (P)	9
				Licence (F)	45
				Total	183

2.3.1.1 Document collection

Two methods of specimen collection were used in this research, and the method was adjusted based on whether the physical documents were examined and imaged, or whether previously captured images of the items were provided digitally by the external research partners.

Physically examined documents

73 of the 183-document set were collected from Sydney (NSW, Australia) police stations in Chatswood, the Eastern Beaches, Surry Hills, and Leichhardt. Within this set of 73 documents, they were mostly NSW driver licences, photocards and some other miscellaneous 'identity' documents, with a smaller number of WA driver licences. There was also a mixture of counterfeit, forged and pseudo documents. All 73 documents were examined with readily available, standard equipment used widely within the field of document examination [43]. Each document was examined with white light and an UV light source (365 nm) before being photographed and scanned at 600dpi using a CanoScan LiDE 400 flatbed scanner and a background canvas, to normalise the colours. This background canvas was developed and provided by our external collaborator at UNIL, Switzerland (example of the canvas provided in Appendix Figure A. 1). Images of the documents under UV light were taken with a Canon EOS750D DSLR camera with a 50mm lens and tripod. These images were then saved onto the secure NSWPF server in accordance with Ethics Approval: ETH204695.

Per ethics approval, personal information was irreversibly redacted from the documents to protect the identity of the document holder using Affinity Designer version 1.10.5.1342. Each document was imported into a template which had black boxes over the areas of the document containing personal information, while still allowing the template text to be viewed. After the redaction boxes were appropriately aligned, the layers of the image were irreversibly compressed into a .PNG file, resulting in a single layered file that was fully redacted. The

editable images (Affinity Designer files) were then transferred onto the secure NSWPF server and any original, unredacted images were deleted from the researcher′s devices in accordance with the ethics approval and data management plan. Only the redacted images were kept and used in the profiling method. Once this process was complete, the physical documents were returned to the police stations they had originated from.

Digital documents (images)

The remaining 110 documents were transferred to the researcher digitally by two Australian law-enforcement organisations. Images of previously seized or intercepted fraudulent driver licences were stored on the servers of these different organisations. These images were irreversibly redacted by these external partners before being securely transferred in preparation for the profiling work. This data set of images contained counterfeit provisional and full (unrestricted) driver licences from NSW, VIC and WA. Most of these documents had been imaged under white light and UV light when they were originally seized, however, the exact image and lighting parameters were not provided. It should be noted that 54 of the Victorian licences (provided by Organisation 3) were not imaged under UV light, so no UV features could be extracted or used in the profiles of those documents. Additionally, all 110 documents were collected using inconsistent image lighting, with some of them having been captured in bright white light, and others having been captured in quite low lighting. In these cases, some features could not be extracted because of the variation in image quality, however, for these documents, other features were simply targeted.

2.3.2 Manual profiling and comparisons

The manual method used in this research was presented in Section 2.1.2, Figure 2.4, with the exception being that no comparison metrics were used due to a lack of information provided about the documents, and there being too few documents of the same types and from known

sources to train a comparison model. After the images of the documents were collected, features of interest were extracted and profiles were created, codified, and then manually compared.

2.3.2.1 Extraction of features of interest

Two main types of features/characteristics were targeted in this analysis, general and specific [17]. The general characteristics are those that comprise the basic features of the document such as document type, fraud type, document numbers, substrate material and its UV reaction. These are characteristics that can be compared across all document types as all documents share them [17]. Specific characteristics, on the other hand, are those that are only shared by documents that belong to the same series, i.e. have been produced by the same source. This includes features relating to the layout and content of the document, logos and security features, and errors or anomalies introduced during the manufacturing process [17] such as ink spots or misprints. To ensure a robust profile was created, both general and specific features, spanning a variety of areas in the document were selected.

As many of the features of interest form parts of the security elements within these documents, an exhaustive list of them cannot be provided, however, things such as the document numbers, fonts, spelling and other mistakes in the template text, styles of security features like UV logos, and styles of other logos and design elements were targeted for this comparison (some examples of the features extracted from counterfeit documents can be found in Appendix Table A. 5, Table A. 6 and Table A. 7) . Contrasting with previous research, the printing methods used in the creation of the documents could not form part of the profiles in this research, as the printing methods could not be reliably identified from the images of the documents due to inconsistent image parameters. So, this feature was not included.

Feature selection

The features that are selected to form the profile invariably impact the types of links and relationships that can be identified between the entities, in this case, documents [14]. After all, when creating profiles of entities, a simplified model is being created that is representative of the entity to facilitate the comparison process, so a conscious selection process must be undertaken when selecting the characteristics to form the profile [14, 170]. As recommended by Baechler et al. [14], the performance of the chosen features forming the profile were examined against a selection criterion. These criteria examined the intrinsic and extrinsic properties of the features, with intrinsic criteria being those that depend on the feature itself while extrinsic are those that are more related to the measurement or observation methods used [14]. Given the number of criteria, it is difficult in practice to satisfy all of them, instead a balance should be struck between intrinsic and extrinsic criteria. Some of the criteria that were used to select the characteristics of interest in this work included (but were not limited to): low intra-variability, high inter-variability, representativeness, comparability, non-destructiveness, accessibility, sensitivity and specificity. For illustrative purposes, only some criteria are explained and the performance of one feature, the state badge (Figure 2-6), is examined in Table 2.4. A more comprehensive list of the different criteria can be found in Appendix Table A. 4, with a larger list of extracted features of interest in Appendix Table A. 5, Table A. 6, and Table A. 7.

Figure 2-6: Example of the state badge from one of the counterfeit licences within the data set

Table 2.4: Description of the criteria developed by Baechler et al. 2015 [14] and the performance of the state badge of the counterfeit NSW driver licences against them. The full criteria have been included in Appendix Table A. 4

Criteria	**Description**	**Performance of state badge (NSW Licences)**
		Intrinsic Criteria
Low intra-variability	No or low amount of variation within a group of traces from the same source	Very little to no intra-variability within the series. One exception was one series which contained two distinct styles. These documents are still grouped based on the other characteristics, highlighting the benefits of the multi-dimensional (multi-feature) profiling approach.
High inter-variability	Significant variation among traces of different sources	Each series was identified as having its own state badge classification, and there was no overlap between series.
Complementarity	The features must be as independent as possible	The style of state badge used doesn't dictate the presence, absence, or style of any other feature.
Representativeness	Reflects the features/characteristics of the source(s)/activity(ies) used to create the document	If the state badge/magnetic strip is bought from an external source and then applied, this reflects the materials used in the manufacture. If it is made on-site, it is representative of the stamp/template used by the source.
		Extrinsic Criteria
Low resource requirement	Low requirements for time, cost, equipment, knowledge, and training	The characteristic can be observed with the naked eye and requires no special equipment.
Accessibility	Equipment and knowledge required to extract/identify the feature are readily	Visual characteristics are highly accessible, and no special training is required to identify the differences between classes.

	available, and the trace is readily available to extract with the correct equipment and knowledge	
Non-destructiveness	Does not alter or destroy the trace	The characteristic requires no treatment or alteration of the trace as it is a visual feature that is perceptible under white light by the naked eye.

The number of features that were extracted from each document was largely dictated by the complexity of the document, i.e. if there were complex or simple design elements, as well as the image quality. The range of features compared within each document type set is included in Table 2.5, if there was a feature missing from a document (i.e. it was not provided or could not be extracted because of image quality), it was not used as a comparison point, and was instead removed from the comparison, hence creating a range of features of interest.

Table 2.5: Document and fraud types and the number of features that were extracted to create the profiles. Note: No features were extracted for the international licences as there were no documents with which to compare them, so that is represented by an 'NA'.

Type of fraud	Type of document	No. of features
Counterfeit	NSW Driver licence	30-47
	WA Driver licence	24
	VIC Driver licence	19-20
	Int. Licences	NA
Forged	NSW Photo cards	1
Pseudo	NSW Student ID	12
	NSW Age Proof	12

2.3.2.2 Creation of profiles, codification, and comparisons

Once the visual features were extracted for each document, they were manually codified to form the document's profile, as shown in Table 2.6. Where features were evaluated as either being present or absent, such as the UV reaction of the substrate and the misspelling of 'document' shown in Table 2.6, a binary system was used, with 1 indicating the feature was present, and 0 indicating it was absent. Other, more complex features were given a number based on the style of the feature, such as the font style and UV feature.

Table 2.6: Example profile conversion from characteristic type to numerical profile. This is an example profile used for illustrative purposes and does not correspond to any of the documents in the specimen set and does not encompass all extracted features of interest.

Characteristic	**Profile (numerical)**
Licence Number	123456
Card number	987654321
Substrate UV Absorb	1
UV feature	6
Template font	2
Misspelled 'Document'	1

When all documents were profiled, a many-to-many comparison was done, using comparison grids, similar to adjacency matrices used in Social Network Analysis (SNA) [171]. During this process, the profile of each document was compared to the profile of every other document of the same type, and the percentage similarity was calculated using the formula as provided below:

$$\%\, Similarity = \frac{Number\ of\ correlating\ features}{Total\ number\ of\ features} \times 100$$

The similarity score was used as a tool to assist in the identification of links between documents, with a similarity percentage threshold of 75% being selected as the cut off. The similarity threshold was calculated based on the number of correlating features between the profiles, divided by the total number of potential features (i.e. 7/10 = 70% similarity), with all features having the same value or weight. If two documents were identified to have a similarity score of 75% or greater, they were identified as being linked. Previous research that has used comparison metrics to conduct the comparison of document profiles has used similarity scores of between 90-100% to establish a link [15], however, as indicated in this and other research, the similarity scores (a.k.a correspondence scores) can be adjusted and chosen by the examiner to suit the aims of the examination [13, 15, 16]. Meaning that more broad examinations aiming to get a general understanding of the structure of the criminal environment can set a lower threshold to limit the number of false negatives, while using multiple, specific features to limit false positives as much as possible [172]. This is particularly useful when considering that the method of comparison (manual or automated using comparison metrics) as well as the size of the data set will dictate what the most appropriate similarity threshold will be [15, 16]. As stated by Baechler et al. “The notion of a threshold should be understood as a dynamic cursor influenced by the definition of what a link means, by the evolution of the problem, and by the needs of the process.” ([15] p. 74).

A lower threshold was selected in this research to ensure that potentially linked documents were not overlooked while reducing false positives as much as possible, as the aim was to investigate a previously unexplored criminal environment and to determine if there was any potential indication of organisation. Of course, in some contexts, credibility (i.e. certainty) is more important, a situation most often encountered within the judicial system. In this context, a false positive can be detrimental, resulting in a false conviction. However, in this work and forensic intelligence more generally, the end goal is not to service the judicial system, but rather

to provide insight into the structure and functions of a complex criminal environment and perhaps provide leads for an investigation. In this context, it is more important to limit potential false negatives, as the potential of "…missing what has to be found (i.e. suffering from an incomplete perception or linkage blindness) …" ([14] p.50) is of greater concern. Whenever a potential link is initially identified, this isn't an assertion of 100% certainty that the link exists between the two entities, but rather is a starting point, a hypothesis that will be further scrutinised and evaluated using alternative information [14]. It is preferable in this kind of exploratory analysis to cast a wider net and ensure that all potential series are identified, rather than the alternative of potentially overlooking series or patterns [14]. Especially when considering that the series and relationships identified can then be confirmed or denied after closer scrutiny.

Research conducted by Baechler et al. [15] (which used the 90-100% threshold) not only had a large enough data set to enable the use of comparison metrics, but also had far more contextual information about the documents that were being examined [15]. It was therefore determined, based on the information that was provided for the documents examined in this research, the aims of the examination and the use of features that were very specific to the documents, that a 75% threshold value would be the best way to establish links while limiting false positives and false negatives as much as possible.

All profiling, codification, and comparisons were completed using Microsoft® Excel® for Microsoft 365 MSO (Version 2404).

2.3.2.3 Analysis

Social network analysis

Social Network Analysis (SNA) focuses on the characterisation of the relationships between networks of connected people, the structures of networks, and the relationships between nodes,

or entities (i.e. individual actors) within said networks [173, 174]. Based on the patterns of the networks it is possible to identify and highlight the organisation of criminal networks, their structure, efficiency, and even their resilience [173]. SNA has been used previously in the examination of the structure of the fraudulent document criminal environment to assist in characterising and comparing the structures and organisation behind this illicit market [13]. In this work, the following SNA indicators have been calculated to assist in the characterisation of the Australian fraudulent document market, and to facilitate comparison between the Australian market and that which has been examined in Europe, as well as previous research into Australian organised crime. It should be noted that the social network analysis in this work was limited to using the average degree and density to assist in the comparisons between the results of this analysis, and previous research. It was not possible to conduct any more in-depth analyses of the social networks of the forgers as the information that would be necessary to conduct this analysis (i.e. the identity of the forger, their associates, mentors etc.) was not available and was therefore beyond the scope of this research.

Average degree

The average degree indicates the average number of links per document, and in combination with the density, helps to illustrate the cohesion, structure, and unity within the criminal market [13]. This indicates how connected the network is, as the higher the average degree, the more connections there are within the network. The average degree was calculated using the formula below:

$$Average\ degree = \frac{Total\ number\ of\ links}{Total\ number\ of\ documents}$$

Density

Density examines the number of links or connections within a network compared to how many links are possible, measuring the extent to which nodes within a network are connected [171, 173]. As the relationships between the documents are symmetrical (i.e. they are undirected and a link between nodes represents a connection), the following calculation was used to calculate the density of the connections within the specimen set [171, 173]:

$$Density = \frac{2L}{n(n-1)}$$

Where L is the total number of links, and n = the total number of nodes (documents), with the numerator representing the total number of links in the network, and the denominator representing the total possible links [13, 171, 173]. The density is often represented as a percentage, with a fully connected network having a density of 100% (or one) while a network with no links will have a density of zero [173, 174].

Quality indexes

Previous research has used the quality of documents to help identify documents and series that constitute a particularly high threat (i.e. they are more likely to fool officials and examiners) [13, 15]. This can assist in the identification of particular sources that are posing a higher level of risk, as well as providing intelligence to front line document examiners and individuals who regularly encounter the documents as to what features should be targeted during the authentication process to ensure there is less chance of being fooled [13, 15]. This can also help document manufacturers and government bodies identify features that need to be developed or changed to more effectively prevent further counterfeiting or forgery [13, 15].

The quality of a document and/or feature was determined by comparing the features within the fraudulent document to the corresponding features of a legitimate document. Each feature was scored based on how well it aligned with the legitimate feature according to Table 2.7.

Table 2.7: Feature scoring categories to determine the quality index of documents. These scores are based on whether someone who is familiar with the document template e.g. a bouncer, but not a document examiner, could identify the feature as fraudulent.

Score	Definition
0	Feature not included or not extractable
1	Feature attempted, but would easily be identified as fraudulent by lay person
2	Only someone highly familiar or trained with the document could differentiate it from the legitimate
3	Feature non-differentiable from the legitimate feature

The key consideration when examining and scoring the quality of a replicated security feature is whether someone who is not a trained document examiner but is reasonably familiar with the type of document could identify the feature as fraudulent. This would include individuals such as bouncers, and bank or post office clerks. Generally, those features that have been allocated a score of 2 may be differentiable from the legitimate version of the feature, but only due to slight differences or small mistakes in its style or reproduction. They would be unlikely to be detected unless very closely examined. Those that have a score of 3 are completely non-differentiable from the legitimate feature if being authenticated by a moderately trained operator using standard equipment [13, 133].

Document quality and average quality per series

To estimate the quality of the documents, the series and the features within the documents, the quality of each document was determined by evaluating the number of security elements and

core design features that were successfully replicated by the manufacturer. This was represented as a percentage of the number of features that were of a high enough quality to be classified as legitimate. The average quality across a document series was then examined.

Feature quality

The quality index for each security or design feature used within the document was examined to see which feature was being the most effectively replicated across the document set, and therefore which ones were the least effective for deterring counterfeiting. This was calculated by identifying the number of documents within the specimen set that had correctly replicated the feature to a high enough quality that it would fool someone familiar with the document features (a score of 2 or above).

2.3.3 Algorithm-based comparisons (Padif)

Some research has explored the benefits of combining the manual human-driven profiling approach (as described in Section 2.1.2) with a semi-automated, more objective comparison relying on the use of image processing techniques and algorithms (Section 2.1.3). The documents examined in this research were compared using the algorithms developed and implemented within the profiling systems used in Europe (ProFID and BIDIF), known as Padif, to firstly establish whether they would assist in the identification of series within the data set, but also to establish if Padif could be applied to these documents and their features. To test this, a small sub-set of the documents (n=26) were uploaded to a sandbox version of ProFID that was only accessible by a restricted number of researchers. This sub-set of documents was chosen as they were the largest group of documents that had been physically examined and therefore were scanned consistently and were of the same document type (provisional NSW licence).

2.3.3.1 Image preparation

To ensure uniformity in the images only images that had been captured using the UNIL background canvas (as outlined in Section 2.2.1.1) could be examined using Padif. To prepare the images for upload into ProFID, two QR codes were generated and then integrated onto the image of the scanned document. The first QR code, which identified the scanner used to capture the image, was generated after entering the scanner brand, model, and serial number into ProFID. The second QR code enabled ProFID to identify what document the scan belonged to, and which side of the document had been captured. To create these QR codes the basic information about the document (such as the document number) was entered into ProFID. Affinity Photo 2 (Version 2.5.3.2516) was then used to integrate the QR codes onto the canvases, and the combined images were then exported as .PNG files and uploaded into ProFID (an example has been provided in Appendix Figure A. 1).

2.3.3.2 Selection of regions of interest

After the document images were prepared and uploaded into ProFID, the regions of interest (ROI) were identified for each document type. The regions of interest are the areas that the algorithm will compare between the different images. An example of potential regions of interest is shown in Figure 2-7. It should be noted that areas that are obscured by optically variable devices (i.e. holograms) should not be targeted, as these can obscure the regions of interest, therefore hampering the comparison. Similarly, areas that contain variable information (e.g. personal information) should not be targeted. The regions of interest that were selected for each analysis is provided in Appendix Figure A. 2 and Figure A. 3.

Figure 2-7: An example of the regions of interest that were selected for one of the Padif analyses.

2.3.3.3 The comparison process and analysis of the results

Within Padif, the regions of interest are compared, pixel by pixel, using three different comparison metrics (Root-mean-squared error (RMSE), Euclidean Distance and Ward)[14] to determine the distance (i.e. difference/similarity) between the different regions of interest, and therefore the documents. To illustrate the variation based on regions of interest, three test analyses were conducted, with each having different regions of interest selected. The results of the analysis are presented as a dendrogram, with the distance between the documents (i.e. the length of the line) illustrating the difference between them. The longer the line, the more different they are. The dendrograms were examined, firstly to identify the groupings that were created by Padif and secondly to see if the Padif results agreed with the groupings that were determined using the manual profiling process. Any anomalies or variations within these groupings were then examined.

[14] Clustering method: Ward
ROI Distance aggregation method: Euclidean distance

2.4 Results and Discussion

To properly understand the Australian fraudulent document criminal environment, the information that can be gathered from the systematic examination and profiling of these documents must be evaluated. Typically, the intelligence that can be gathered from this process is divided into three different levels depending on the size of the dataset, the depth of examination required and the level at which the intelligence can be applied e.g. single-case, multi-case or the broader criminal environment (Section 2.1.1). To establish and illustrate how this systematic forensic intelligence method can be applied to these different intelligence levels, the results in this chapter will be divided according to their level. In this research, no contextual information was provided about the documents that were examined, which meant that the interpretation of the results was somewhat limited. It was not possible to verify the linkages through examining those known to originate from a single source, or to identify temporal and spatial trends in manufacture, distribution and use of the documents. For this reason, this analysis is limited to the surface/strategic and M.O./operational levels.

2.4.1 Surface or strategic level

The surface or strategic level of analysis has a very broad focus, aiming to provide a greater understanding of the overall criminal environment, focusing on specific criminal activities and their evolution over time [150]. At this level, very basic analysis can provide useful information regarding the types of documents that are being encountered, and if the contextual information about their seizure has been documented this can be combined with the analysis of trends in their manufacture and distribution over time. Because of the more general nature of this analysis, the types of features required are the easiest to extract, being the general features of the document such as document type, issuing country, and type of fraud [15].

As illustrated in Table 2.3, across the whole specimen set, NSW documents are the most represented, followed by VIC documents, likely due to the potential bias occurring as the organisations from which the documents were collected were based in NSW, the ACT and VIC.

When looking at the forgery types within the specimen set, the majority (88%) of the documents were counterfeit driver licences. The remaining fraud types, being forgeries and the pseudo documents, made up 10% and 2% of the specimen set, respectively. These proportions are not too dissimilar to what was found in Switzerland, where 64% and 19% of the documents seized were made up of counterfeit and forged documents respectively, with all other fraud types falling below 10% of seizures [175]. These numbers are also in line with what has been found internationally [176]. Generally, plastic credit card-style documents, are easier to counterfeit than to forge because of the embedded security features that are designed to make the documents tamper-proof, such as security laminates [13, 51]. It has also been argued that counterfeited documents are generally easier to detect than forged or stolen blank documents [51], which may also contribute to the overrepresentation of counterfeit documents.

It is clear within this specimen set that driver licences are the most encountered document type. Globally, driver licences have been identified as one of the most common products for sale within the international online marketplace for fraudulent documents, making up 73% of the products available for sale [47, 51]. Understandably this has made them a particular point of interest within the document fraud criminal environment, particularly from an intelligence perspective. The prevalence of these documents is likely attributed to the use of driver licences as proof of identity in several countries such as Australia, Canada, and the U.S. coupled with the fact that they contain valuable personal information such as name, date of birth (DOB), and address. This has made them a common target for identity crime and document fraud, internationally, and here in Australia, with driver licences being the most targeted document

type according to the results of the Australian Institute of Criminology's (AIC) identity and misuse reports from 2017 through to 2023 [29-31, 47]. Undoubtedly, further contributing to the prevalence of driver licences within Australia is the fact that individuals do not require their passport or ID to travel throughout Australia, which is something that is required when travelling around Europe. While some international licences were captured within the specimen set, soon after collecting these documents, it was determined that Australian driver licences would be the focus for the remainder of the project, as this was the most prevalent document type encountered by our industry partners.

In most cases, the documents were collected during regular inspections of licenced venues (those that serve alcohol). During these checks, establishments will often surrender any fraudulent identity documents that have been seized by bouncers when "carding" individuals, i.e. checking their identity documents to ensure that they are over the legal drinking age [177]. While a very useful source of fraudulent documents, information regarding the date and location of these handovers is not recorded, and in many cases, the documents are destroyed, reducing any potential examination that could be carried out from an intelligence perspective. For the NSW licences provided by Organisation 1 (n=35), it was possible to identify the year in which the documents were seized as the case number was included in the image file names. From these case numbers, it was possible to get a very partial insight into Organisation 1's seizures of NSW driver licences across the 2016-2021 period.

Most of the licences with a year of seizure (69%), were seized in 2019. Twenty of these documents were intercepted in the post as part of a single shipment entering Australia from Indonesia. Unfortunately, this is a very limited snapshot of just some of the documents that were seized by this government organisation, as more detailed contextual information was not provided with the documents, and in some cases not collected. This is just an illustration of the way that contextual seizure information could be used to help inform on trends regarding

manufacture, use, and distribution of these documents. Understanding this temporal and spatial element of the document fraud criminal environment is important, as has been previously illustrated by international research [13], however, there is not enough data to make any solid conclusions for the documents examined here.

Without exact dates and locations of seizures, and no information regarding what led to their interception or seizure, what can be gathered within this surface intelligence level is limited to examining the fraud type of the documents collected, with some admittedly limited and flawed general discussion of the seizure dates that were surmised from the case numbers of 35 of the documents. To perform proper temporal and spatial analysis of the criminal environment, including identifying trends in the manufacture and distribution of these documents, more detailed information needs to be gathered and subsequently shared regarding the circumstances of these document seizures.

2.4.2 M.O. (operational) level

To evaluate the M.O. level, a higher depth of examination is required focussing on the profiling of the visual features of the documents to identify those anecdotal cases of crime and those that are being carried out by more prolific offenders. The features that are targeted at this level are those that reflect the M.O. used to create them as illustrated in Figure 2-1 and Figure 2-2 in Section 2.1.1.

2.4.2.1 The structure of the criminal environment

Out of the 183 fraudulent and counterfeit documents examined, it was identified, through the manual comparisons, that 172 (94%) were linked to at least one other document, and 17 series emerged. Links were established based on the percentage similarity of the documents, as discussed in Section 2.2.2, with the linkage threshold being 75%. It should be noted that while some documents may not share 100% of their features, their similarity is identified using

features that are so specific to the manufacturing process that a similarity of 75% (or in some cases, lower) cannot be explained by any hypothesis, other than the documents originating from the same source [15]. Furthermore, given the specificity and number of features being compared (especially for the NSW licences) it was deemed unlikely for two documents to share this many features based on random chance. For the NSW driver licences a similarity of 75% equates to a minimum of 30 correlating features, for the VIC driver licences it equates to 18 features, and for the WA driver licences this equates to 15 features. Before this research, part of which was published in 2022 [172], there were no studies that examined the Australian fraudulent document market and fraudulent documents in Australia were, in most instances, treated as isolated cases of document fraud. However, Table 2.8 illustrates that over 90% of each document set examined, except for the international licences, are linked to at least one other document, illustrating that the market for fraudulent documents in Australia may potentially be structured, and not composed of numerous isolated cases as previously hypothesised.

Table 2.8: The number and proportion of the document set with 0, >0, 1-5, etc. links to other documents within the document types studied. Also included in this table is the number of features (or range) compared for each document type along with the total number of links identified within each document set. The average degree and density illustrate the structure and interconnectedness within the networks. The structure of this table was inspired and adapted from Baechler et al. 2012[15]

			Number and proportion (%) of documents with 0, 1, 2, n, links to other documents								
Type of document	Features compared		0	>0	1 to 5	6 to 10	11 to 15	>15	Total links	Average degree	Density (%)
NSW driver licences (n=68)	40-47	Number	4	63	22	14	0	27	450	6.6	20
		%	5.9	94.1	33.8	20.6	0.0	39.7			
VIC driver licences (n=70)	24	Number	1	69	0	0	15	54	1534	21.9	64
		%	1.4	98.6	0.0	0.0	21.4	77.1			
WA driver licences (n=19)	20	Number	1	18	11	7	0	0	32	1.7	19
		%	5.3	94.7	57.9	36.8	0.0	0.0			
NSW photo cards (n=18)	1	Number	0	18	8	8	0	0	40	2.2	26
		%	0.0	100.0	44.4	44.4	0.0	0.0			
Int. driver licences (n=4)	NA	Number	4	0	0	0	0	0	0	0.0	0
		%	100	0	0	0	0	0			
NSW pseudo documents (n=4)	12	Number	0	4	4	0	0	0	6	1.5	100
		%	0	100	100	0	0	0			

Furthermore, a high percentage of the specimen set examined in this research are linked to 15 or more other documents (39.7% of the NSW licences and 77.1% of the VIC licences), which is higher than that of previous research [13]. This suggests that the Australian fraudulent document market may be both organised and punctuated by prolific offenders. It also suggests that larger networks may potentially be contributing to this criminal problem, like what has been found internationally [13, 15, 143].

Social network analysis, specifically the average degree and density measures, can help illustrate the structure of the fraudulent document market, with the average degree corresponding to the average number of links per entity, in this case, per document [13]. The density on the other hand illustrates the proportion of the network that is connected compared

to the total possible number of connections that could exist within the network [13, 173, 178]. The average degree and density have been included in Table 2.8.

When looking at the results for the Australian documents, they suggest that the Australian fraudulent document criminal environment may be structured, with the highest concentration of connections occurring within the markets for VIC driver licences and NSW photocards and driver licences (density of 64%, 26% and 20% respectively). However, before any concrete statements can be made regarding the state of the Australian document market, it must be evaluated whether this high degree of connection is due to the structure of the market, and perhaps the geographical isolation of Australia, or if biases in the document set may be inflating the results.

In 2016, Baechler et al. [13] examined the links and density of the markets for Portuguese ID cards (n=170), French ID cards (n=129) and French passports (n=64). In this analysis, the density of these three document sets was found to be 1.9%, 3.9%, and 3.5% respectively. The most obvious difference between the data set examined by Baechler et al., and that examined here is the size, but even when comparing the document set that was a similar size, being the French passports (3.5%), the density is far greater for the Australian documents. These results could potentially indicate a higher degree of organisation and structure within the Australian document market but are more likely due to the difference in seizure circumstances. While the documents examined by Baechler et al. were seized across different jurisdictions in France and Switzerland across a period of twelve years, those examined here were seized solely within Australia, across an unknown period.

The density of most of the identified networks within the Australian document market seems to be of a similar magnitude to other previously researched criminal and terrorist networks [173, 179-181]. However, the density of the VIC licence market (64%) is much higher. This

can likely be attributed to the comparatively small specimen set examined within this research, combined with the decreased variety of sources. Of the 70 VIC licences examined, 69 of them were connected to at least one other document, and only two series were identified, which of course has led to a highly dense network structure. Only two organisations significantly contributed to these data sets, with all VIC documents provided by Organisation 3 (n=54) being linked, creating the largest series within the data set.

While the large disparity between the densities identified here and previous research is undoubtedly due to the reasons mentioned above, there is the potential that a more significant domestic Australian market may be partially contributing to these higher levels of connectedness. In comparison to European countries such as Switzerland and France, Australia is far more geographically isolated. This, in combination with increased border controls and security, may be contributing to an increased domestic market, much like what has been seen in other illicit markets, such as that for illicit drugs [104, 117]. Undoubtedly, if the Australian fraudulent document market has a high percentage of domestic contributors, this would likely contribute to an increased density of the identified networks. Unfortunately, given the size of the data set examined here, and the lack of contextual information provided around the documents, the conclusions that can be drawn are limited.

The more quantitative results in Table 2.8 are complemented by visualisations such as that presented in Figure 2-8 which shows the overall market structure for the Australian counterfeit driver licence dataset, with each line indicating a similarity between the two connected documents, and clusters of connected documents illustrating a series. It is clear from Figure 2-8 that the largest series is that of VIC_DL1, which is composed of the 54 Victorian driver licences from Organisation 3. Within this series, almost all the licences are connected, creating the dense cluster that is seen in the figure. On the other hand, the second largest series, NSW_DL1 (31 documents) has a subset of documents (n=4) that are less connected than the

rest of the series. These four documents, while still part of the overall series, have some slight differences when compared to the rest of the series, resulting in that slight separation that is evident in the figure. Both series account for a large portion of the counterfeit VIC and NSW driver licence market examined here (77% and 46% respectively), indicating that these sources, if neutralised, may decrease the number of counterfeit documents making their way to consumers.

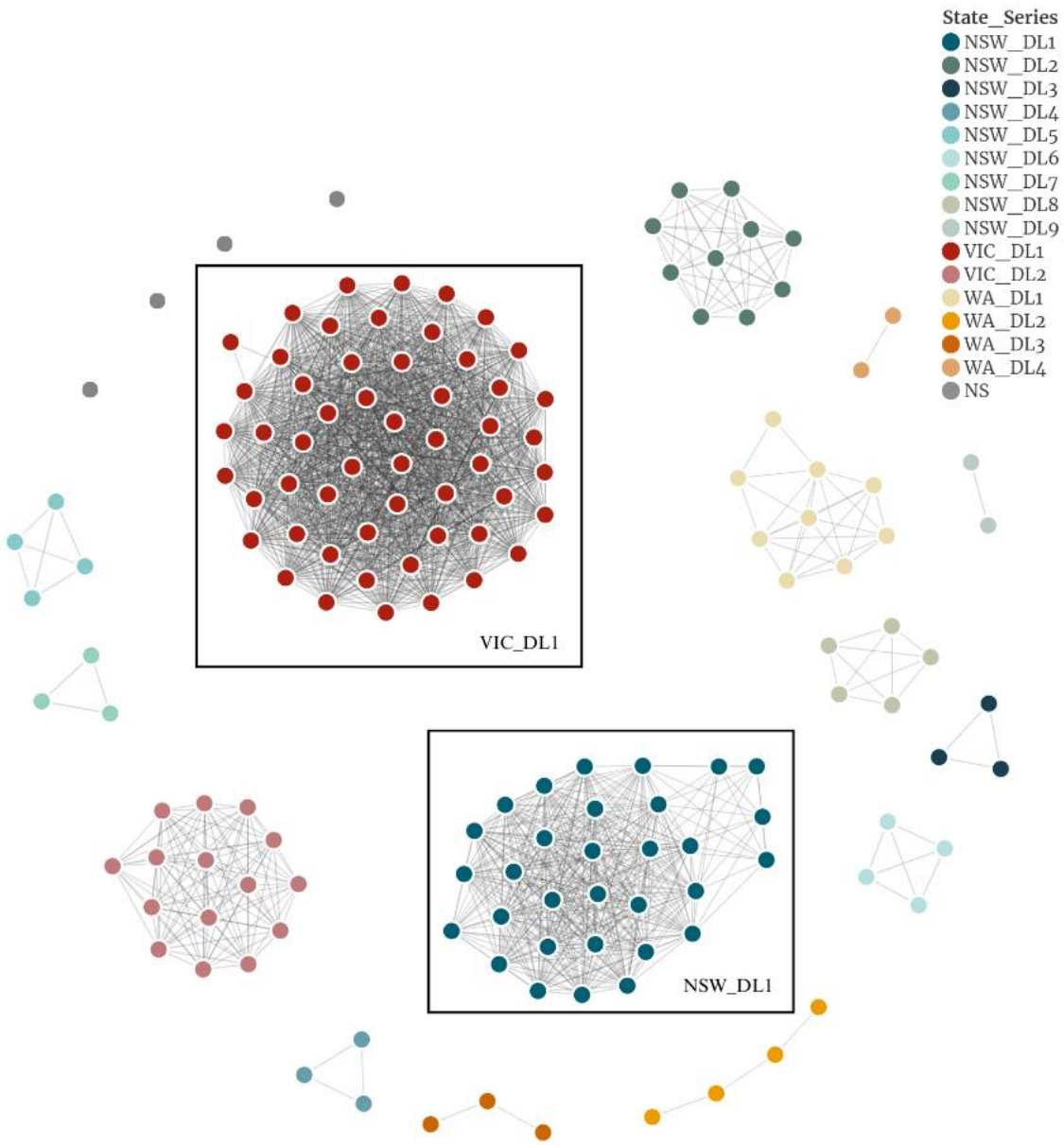


Figure 2-8: Visualisation of the relationships between the Australian driver licences, including those that were linked, as well as the four unlinked documents as indicated by "NS" in the legend (No series). According to the exhaustiveness rule, any unlinked documents form their own class [15]. Each circle represents one document, with the line between indicating a link between those two documents. Each cluster of linked documents is indicative of a series of documents, i.e. those likely produced by the same source. The two largest series, VIC_DL1 and NSW_DL1 have been labelled.

Based on the quantitative and visual analysis, the Australian fraudulent document market seems to potentially exhibit characteristics that have previously been identified in organised and structured document fraud markets [13, 15, 143]. Even if the organisation seen within this data set is inflated due to the size of the data set and a lack of diverse sources, there is likely some

degree of organisation present within the Australian document market given what has been found internationally [13, 15, 16, 32, 143] and the organised crime climate in Australia [166-168, 182-186]. Between 2015 and 2021 the cost of serious organised crime in Australia increased from $36 billion to $60.1 billion [139, 187], and is likely to continue increasing alongside access to and developments within digital and communications technology [139, 166]. While in Australia organised crime activities tend to be camouflaged within the community [166], a considerable number of organised crime groups have been recognised, including outlaw motorcycle gangs (OMCGs) [168, 185, 188], ethnic-based crime groups, family-based crime groups, groups created through a common origin i.e. prison-based groups [167, 189] as well as those involved in the illicit drug market [183], human trafficking and sexual exploitation [184, 190, 191]. As an example, in 2023 a research paper examined 587 organised crime groups involved in drug trafficking that had been previously identified by Australian law enforcement agencies [183]. This was just one analysis and did not consider groups involved in other forms of organised crime.

As indicated by previous research, organised crime and document fraud are often linked, with document fraud considered to be an enabler of almost all serious and organised crime [32]. In 2017, this relationship between the document fraud market and organised crime within Australia was exemplified after a joint New South Wales Police Force (NSWPF) and Australian Federal Police (AFP) operation identified 1,710 falsified documents belonging to an identity document fabrication syndicate [47, 192]. Police successfully tied these documents to 29 organised crime groups and 13 outlaw motorcycle gangs who had used the documents to illegally move $57 million offshore [47, 192]. Police also identified that several other activities had been facilitated using these false identity credentials including hundreds of online scams, visa fraud and the movement of suspected terrorists [47, 192].

While these results indicate (as illustrated in Figure 2.8), that the Australian fraudulent document market may be both organised and structured and that, according to previous research, organised crime is present and flourishing within Australia [47, 167, 168, 183-185, 188-192], more concrete ties between these organised criminal enterprises and the documents examined here cannot be identified due to the size of the data set and the lack of contextual information about the documents. Baechler et al.'s [15] visual profiling method, which was adapted for this research, has been successfully applied to fraudulent identity documents in Europe and has assisted in the identification and subsequent dismantling of criminal networks [37]. Given the Australian organised crime climate, and the degree of connectivity within the documents examined here, it is suggested that this method, if integrated into operations, could assist in understanding and disrupting the activities of organised crime groups in Australia through assisting in the identification of priority targets and in the effective allocation of resources. However, this research is just the first of many steps required to move towards that end goal.

2.4.2.2 Counterfeit driver licences

Most of the examined document set was composed of counterfeit Australian driver licences and within that set, fifteen series emerged, the two largest of which, NSW_DL1 and VIC_DL1 were made up of 31 and 54 documents respectively, as illustrated in Table 2.9.

Table 2.9: The number of documents in each of the fifteen series identified within the counterfeit driver licence specimen set with their percentage similarity ranges (% of correlating features) using the 75% similarity threshold

Document type	Series code	No. of documents	% similarity range
NSW driver licence (n=68)	NSW_DL1	31	75-100%
	NSW_DL2	9	83-98%
	NSW_DL3	3	94%
	NSW_DL4	3	80-98%
	NSW_DL5	4	80-100%
	NSW_DL6	4	95-100%
	NSW_DL7	3	100%
	NSW_DL8	5	80-90%
	NSW_DL9	2	97%
VIC driver licence (n=70)	VIC_DL1	54	79-100%
	VIC_DL2	15	79-100%
WA driver licence (n=19)	WA_DL1	4	75-90%
	WA_DL2	9	75-90%
	WA_DL3	3	75%
	WA_DL4	2	80%

It was found that documents with more complex security features, design elements and templates were easier to profile, in that the more complex a feature is, the greater variation there will be when different manufacturers try to replicate it. Within both the NSW and the VIC subsets, there was no characteristic overlap between the different series, with each series having a unique set of characteristics. This clear delineation between the series was not present within the WA licences. While they still had 24 extractable characteristics, these were of a much lower complexity, which meant that there was less possible variation in the way they had been manufactured. This resulted in a few of the identified series sharing some level of similarity across their different features.

The higher number of series identified in the NSW documents could indicate that there are more distinct operators contributing to the market for NSW counterfeit documents. However, this research is based in NSW, and there was a larger variety of sources for these documents than for the other states, with variation in organisations providing the documents, and a variation in the locations they were seized and intercepted. So, this larger number of series is likely correlating to this increased variation in specimen collection due to bias within the data set caused by the limited availability of documents.

90% similarity threshold

For comparison, the degree of connection for the licences was investigated when the similarity threshold was increased to 90% (as was used in Baechler et al. 2012 [15]). When using the 90% similarity threshold it was found that across the whole driver licence document set 80.9% of the documents were linked (127 of the total 157) and 13 series emerged. The series numbers, along with the number of linked documents and the percent similarity range has been included below in Table 2.10.

Table 2.10: The number of linked documents per series when abiding by the 90% similarity threshold. The range of the percentage similarities for each series has been included.

Document type	Series code	No. of documents	% similarity range
NSW driver licence (n=68)	NSW_DL1	29	90-100%
	NSW_DL2	7	91-98%
	NSW_DL3	3	94%
	NSW_DL4	2	98%
	NSW_DL5	3	100%
	NSW_DL6	4	95-100%
	NSW_DL7	3	100%
	NSW_DL8	3	90%
	NSW_DL9	2	97%
VIC driver licence (n=70)	VIC_DL1	53	92-100%
	VIC_DL2	13	92-100%
WA driver licence (n=19)	WA_DL1	2	90%
	WA_DL2	3	90%

Of course, the most obvious difference is when comparing the results of the WA licences between the two thresholds. As discussed earlier the WA licences had the fewest extractable characteristics which for the most part resulted in the identified series having lower percentage similarities. However, it was determined that the 75% threshold was suitable, particularly for the WA licences as those within WA_DL1 (4 documents with the 75% threshold) and WA_DL2 (9 documents with the 75% threshold) were linked based on an eight-digit serial number that was visible on the documents. As an example, document FLWA_453 and FLWA_268 had a percentage similarity of 75%, but they shared the same document serial number. In fact, the only features that they differed on was a slight variation in alignment of the template text and microprinting, the UV reaction of the substrate and the colour of the UV security feature. These differences can be explained by updates in the UV security feature to make it more in line with the legitimate document or could be an indication that the source

used a different substrate. Either way, for this examination, the 75% threshold was deemed appropriate as it limited false negatives as much as possible and given the aim of this examination was to get a broad understanding of a previously unexplored fraudulent document market, it was deemed more important to avoid false negatives. The presence of false positives was mitigated as much as possible through the selection and inclusion of very specific visual features. The results of the 90% threshold illustrate the versatility of this method and emphasises the high degree of visual similarity between the documents examined in this research.

NSW

There is a general assumption in Australia that fraudulent identity documents, particularly driver licences are being used by underage individuals to gain access to alcohol and other restricted services. Interestingly, 40 of the 68 NSW driver licences examined were for individuals claiming to belong to the 18–25 age bracket, which may be supporting this assumption. However, the Australian Bureau of Statistics identified that 14.2% of offenders of all crime types in Australia are between the ages of 20–24, with 15–29 years olds making up 42.4% of the offenders in the 2020–21 financial year [193]. Therefore, the purchase of alcohol is just one possible hypothesis and does not negate the possibility that these licences were used in the pursuit of other criminal activities. Beyond this, it is also important to consider that a single manufacturer or source could be supplying documents for a range of individuals and purposes [51]. Within the NSW_DL1 series, nine documents (provisional licences) were collected within NSW from licenced venues, but twenty of them (full licences) were intercepted in the mail entering Australia from Indonesia. All twenty of these documents had the same photograph of the individual with different names and addresses, which may suggest that they were less likely to be used for access to alcohol and other restricted services.

As illustrated in Table 2.8, the NSW licences had roughly double the number of extractable characteristics when compared to the other licences examined in this study. Not only did they have a higher number of discernible security features, but the security features and the general design elements of the document were far more complex. This made it easier to identify different series, as there were very clear delineations between them, with very little to no overlap, perfectly illustrating the theories postulated by Baechler et al. in 2012 [15]. The traces left on these fraudulent documents (visual features) are clearly a reflection of the forgers M.O. which is based on their materials, equipment, methods, and biological characteristics [15]. Within the NSW documents, a key feature that the manufacturers attempted to replicate was the microprinting[15], and an example of the legitimate NSW microprinting has been included in Figure 2-9.

Figure 2-9: An example of the legitimate microprinting from the NSW driver licence

Figure 2-10 shows six different examples of the microprinting identified throughout the NSW series. Because of the manufacturers difference in methods, techniques, equipment and materials, they have all produced very different results. This key premise upon which the international profiling method relies is clearly applicable to the counterfeit documents

[15] Microprinting is essentially printing that is so small it cannot be easily replicated as it requires the use of specific printing processes such as offset printing.

encountered in Australia. This, in combination with the identified structure as illustrated in Figure 2-8 supports the hypothesis that a systematic profiling method for fraudulent identity documents could be implemented in Australia, and that it would assist in the identification of prolific offenders and would help to illuminate this previously shrouded criminal environment.

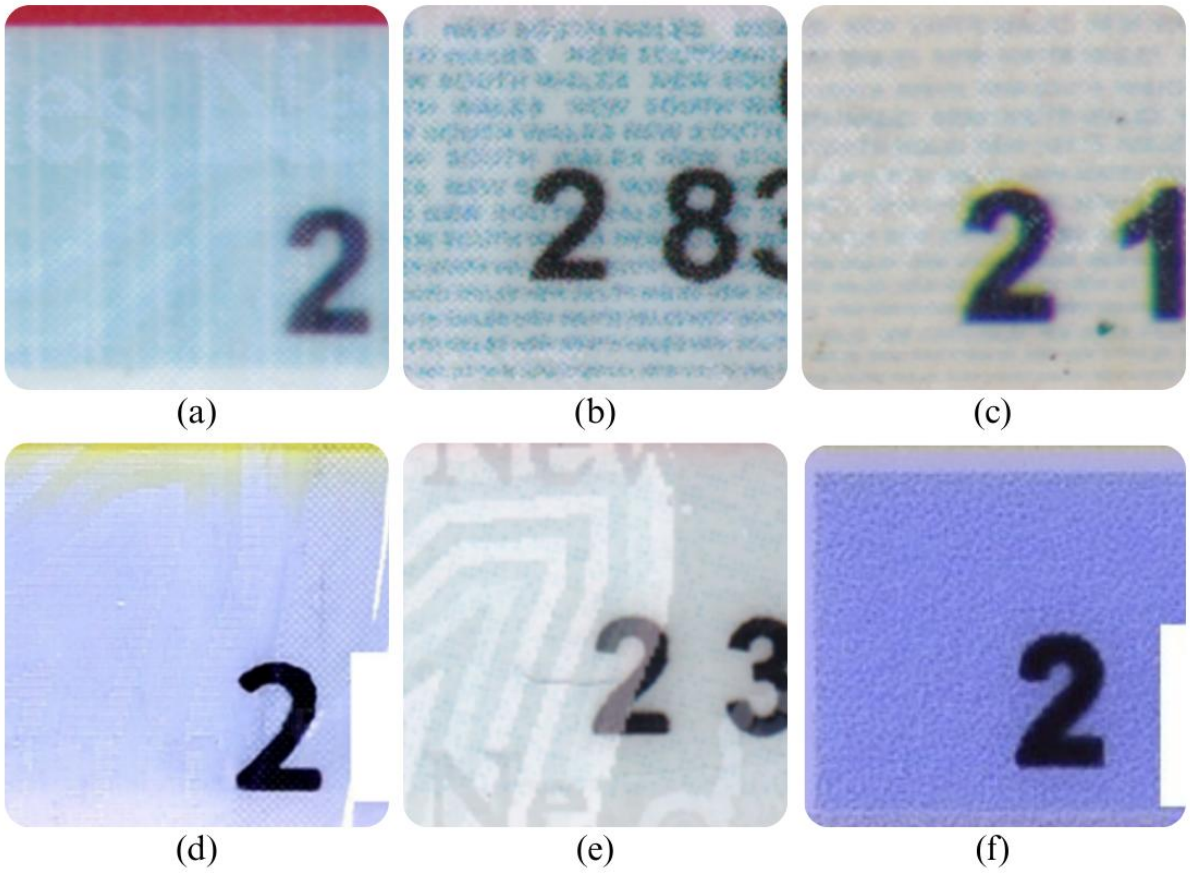


Figure 2-10: Examples of the different microprinting styles encountered within the counterfeit NSW driver licences. In order from (a) to (f) the series that each style appeared in was NSW_DL1, NSW_DL2, NSW_DL3, NSW_DL4, NSW_DL5 and NSW_DL6.

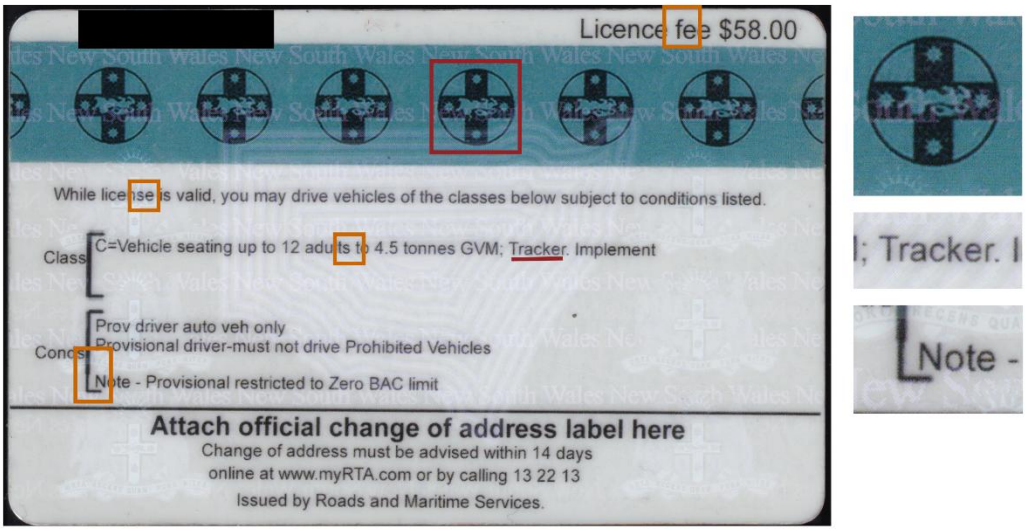
The identification of the structure of the criminal environment is not all that a systematic visual profiling method can provide. With contextual information around the documents being examined, such as seizure dates, locations, and associated criminal activities, trends in the manufacture, distribution, and use of the documents can be identified [13, 15, 51]. This can

assist in the generation of relevant intelligence alerts regarding emerging document types, understanding adjacent criminal activities that have been enabled by document fraud, and the identification of advancements or developments of M.O. While in this research, minimal information was provided about the documents being examined, a pseudo-temporal and spatial analysis was conducted using the NSW counterfeit licences.

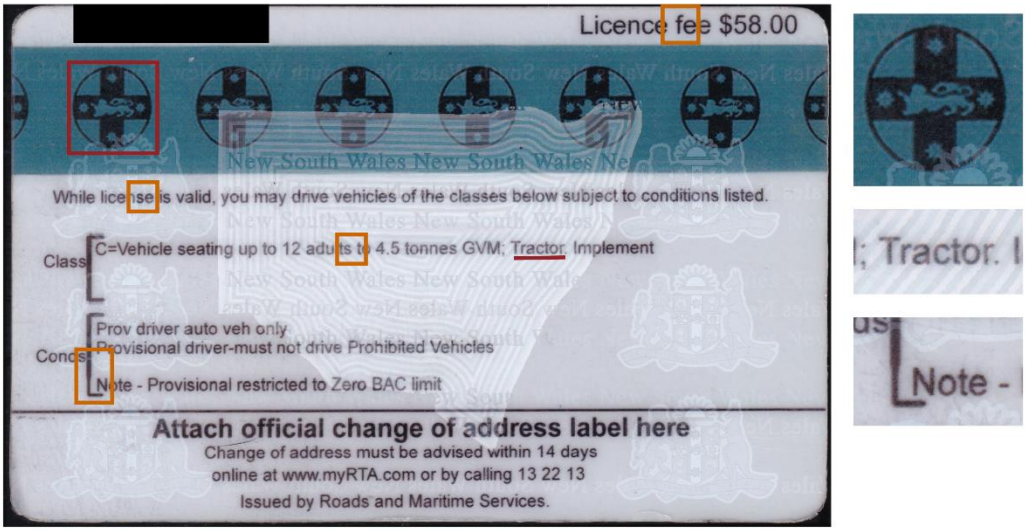
Temporal analysis

As all dates within a document (e.g. the date of issue and expiry) can be easily fabricated, previous research has analysed the date of seizure of a document as a pseudo indicator of its manufacture date [13]. This date, in combination with the visual analysis of a document's features can enable the evaluation of M.O.s over time, providing an indication as to when particular M.O.s are active and if/when they have changed [13]. This is of course entirely reliant on having access to the seizure information for each document. However, even without this information some hypotheses can be made based solely on the features themselves.

As illustrated in Figure 2-11, the back of the NSW licence has an area that is quite text-heavy, as it contains the conditions related to the use of the licence. While not visually complex, this concentration of text and formatting creates many opportunities in which the forger may make mistakes. Both documents in Figure 2-11 are from series NSW_DL2, and seven of the nine licences within this series share the typo of 'Tracker' as illustrated in (a), and the inverted state badge lion. The other two licences in the series look like (b) with both the 'Tracker' typo and the inverted lion corrected, meanwhile ignoring other, smaller mistakes such as the use of the American spelling of 'license'. This is a good indication of the theories postulated by Baechler et al. that, following rational choice theory, manufacturers will only make changes when necessary, such as to correct noticeable mistakes or to keep up to date with developments in the security features of the documents [13, 15].



(a) Licence with "Tracker" and State Badge errors



(b) Licence with errors corrected

Figure 2-11: The backs of the cards from series NSW_DL2 illustrating the errors present within seven of the nine licences (a) including the misspelling of 'Tractor' and the inversion of the lion in the state badge (highlighted in red), with the corrections that have been made highlighted in red in (b). Other mistakes that have not been corrected are indicated in orange.

Another potential M.O. development is seen in Figure 2-12 which shows two microprinting styles identified in NSW_DL1. All licences, except for one, exhibit the streaky microprinting style (b) while one document had the grid style shown in (a). Upon closer examination, it appeared that the spaces between the grids of 'NEW', 'SOUTH' and 'WALES' of style (a) were quite consistent, and upon overlaying both styles it was found, as illustrated in Figure

2-12 that the gaps and spaces align between the two styles, supporting the hypothesis that they are linked. It is possible that the streaky style (b) may be the results of repeatedly scanning and reproducing the grid style (a) resulting in a decrease in quality, or that the grid style has grown from the streaky style in the forgers attempt to make the microprinting of their document closer to the legitimate version.

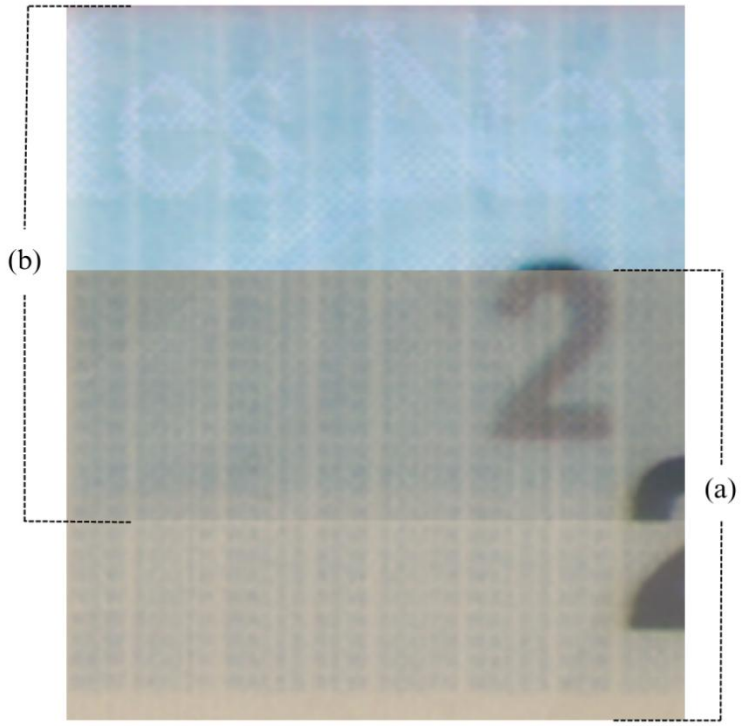


Figure 2-12: Overlaid image of microprinting styles (b) and (a) to illustrate the similarity in placement and alignment of the different elements within the microprinting. Both these styles of microprinting were present within NSW_DL1.

Of course, without the seizure information, the potential developments in Figure 2-11 and Figure 2-12 are just conjecture based on the high degree of similarity between the documents within the series, and the logical assumption that the documents would be developed to reduce the errors as opposed to the opposite. If more contextual information was gathered for these documents, it would be possible to verify these and any other developments in M.O. and to understand shifts or changes to the Australian criminal environment over time. Even with the

obvious limitations, the information presented in Figure 2-11 and Figure 2-12 proves the ability of the method to still detect links across (suspected) updates of M.O. This suggests that this method would successfully be able to link Australian documents across extended periods, as has been done internationally [13].

Spatial analysis

Spatial analysis of the document market has proven to aid in the identification of trans-jurisdictional and transnational document series, and thus in turn, organised crime networks [13, 37, 143]. Given that both organised crime, terrorism and identity crime are not limited by borders, it is reasonable to assume that the fraudulent document market would also be similarly without restrictions. While an extensive spatial analysis is reliant upon having more detailed seizure information, given the information that was provided for the documents in this specimen set, a more general, quasi-spatial analysis can be conducted based on the examination of cross-organisational links. The NSW driver licences are used here as an example, and each of the five organisations (Organisation 1 and the four area commands of Organisation 2, i.e. NSWPF), are treated separately. This is to illustrate the very separate attitude often adopted by policing agencies when dealing with fraudulent identity documents, and to illustrate that prior to this research no combined analysis or communication between departments was undertaken in relation to these documents. After the application of the profiling method and the systematic comparisons of the profiles it was found that 34% of the links across the NSW licence set and three of the nine series were exhibiting cross-organisational links as illustrated in Figure 2-13. The most significant of these cross-organisational links were in series NSW_DL1, where nine of the documents from Organisation 2 area SH (Org 2_SH) were linked to 22 documents from Organisation 1. As mentioned previously, 20 of these documents from Organisation 1 were intercepted as part of the same seizure that was entering Australia from Indonesia. This

suggests a potential investigative connection between documents encountered in Australia and a potential international source.

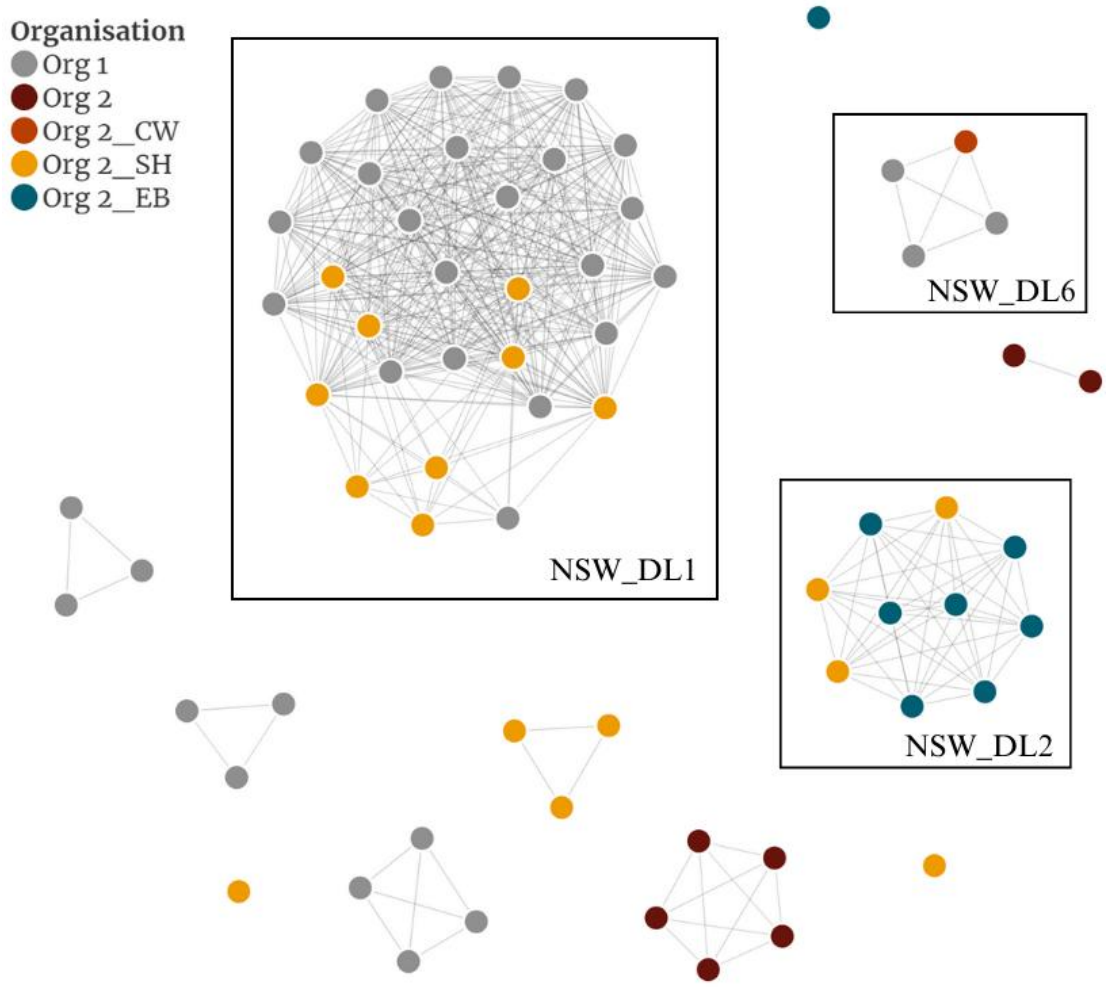


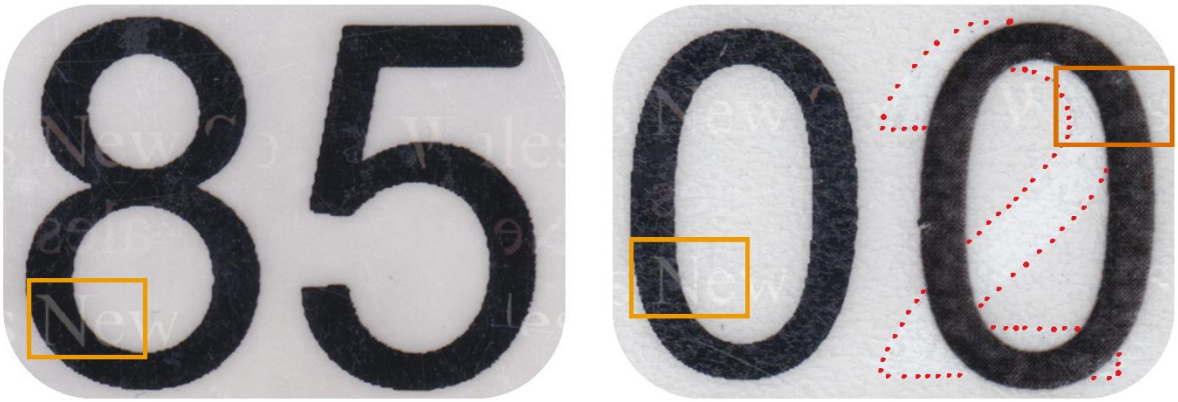
Figure 2-13: Cross-organisational links identified within the NSW driver licences specimen set. The organisations are indicated by their different colours. All the grey documents were those from Organisation 1. The three series that have cross-organisational links have been highlighted.

Organised crime groups will quite often operate across state and territory borders, with Morgan and Dowling identifying in their 2023 analysis that 48.2% of the 587 organised crime groups they examined were operating in more than one Australian state or territory [183]. This

tendency for cross-border operations of organised crime networks, coupled with the cross-organisation analysis presented here makes it clear that greater communication and information sharing is needed between organisations and across different state jurisdictions to not only properly combat the document fraud criminal environment, but also to more accurately understand the structure of and key sources within the market. The current siloed attitudes towards the document fraud criminal environment, and the lack of information sharing, contributes to linkage blindness [153] and the misconception that the fraudulent document market is unstructured and composed of isolated cases.

2.4.2.3 The forged NSW photocards

NSW photo cards are used in most cases as a proof of age card when an individual does not have a driver licence. They have a very similar structure as the driver licence, being a plastic credit card style document with an overlaid transparent laminate that contains the optically variable device (OVD). All the forged documents within this specimen set were altered using the same method, where the laminate over the area containing the DOB was lifted and the year of birth was then scratched off. The original laminate was then replaced, and a second laminate was added on top containing the new year of birth. An example is included in Figure 2-14, which shows an original, unaltered document (a), next to an altered example (b). In an unaltered document, the OVD appears over the printing of the DOB, however, in the forged documents, the printing is on top of the OVD layer, indicating that a second laminate has been added on top. This was also confirmed through taking apart one of the licences and examining the different layers.



a) Legitimate DOB b) Altered DOB

Figure 2-14: Comparison between a legitimate DOB from an NSW photocard (a) and the DOB of the forged photocard (b). The original DOB has been scratched off, but it is still visible by examining the void space as highlighted in red. The areas where the OVD is overlapping the printing are highlighted in yellow, and the void space where the OVD is missing from the altered print space is highlighted in orange.

As the forgery of the document was limited to the alteration and addition of one key visual feature, the number of features that could be examined and profiled was therefore quite limited. When examining the documents it was noted that the forger made a choice as to whether one or both digits of the date of birth were scratched off and reprinted, and then the style of printing that was used to print the new date of birth. Figure 2-15 shows the three different identified printing styles. Based on the visual characteristics of the printed numerals on the replacement laminate, seventeen of the eighteen documents were organised into three potential series as illustrated in Table 2.11, with only one document not being classed into a series as the fraudulent printing had been fully removed. The percentage similarity was not shown for each series as too few features were used in the profile so the percentage would not be an accurate indication of the similarity.

Table 2.11: Number of documents per series for the forged NSW photocards

Series code	No. of documents
NSW_PC1 [Rough]	7
NSW_PC2 [Scaled]	4
NSW_PC3 [Smooth]	6

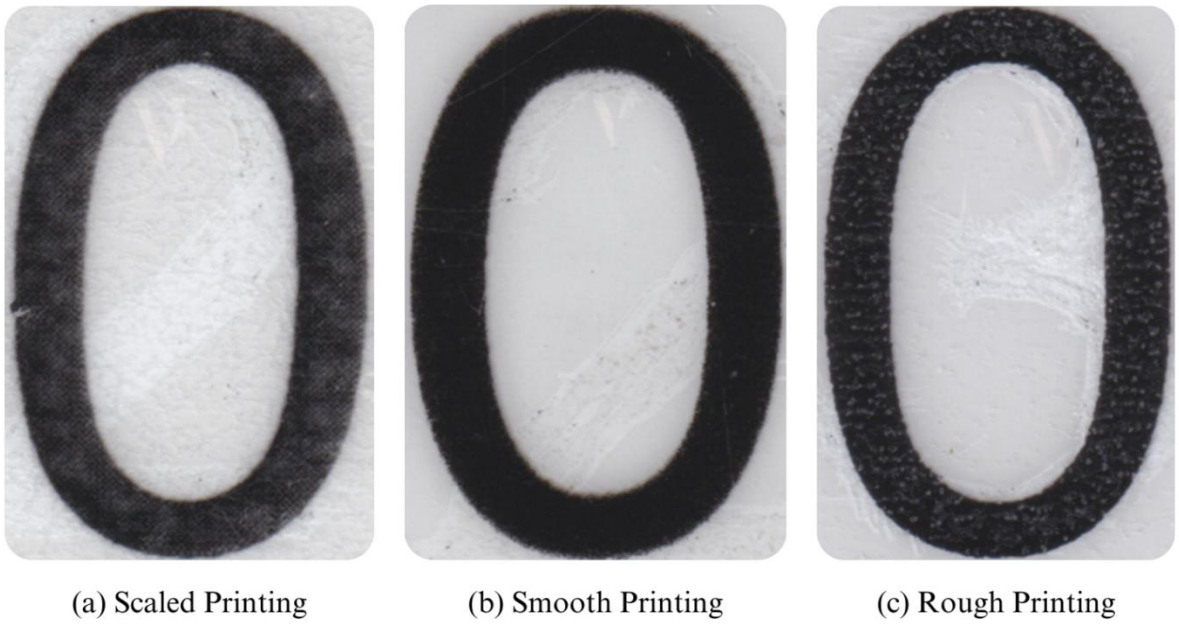


Figure 2-15: The three different identified printing styles used on the forged photocards that have been divided based on their physical appearance, (a) scaled, (b) smooth and (c) rough

While admittedly the use of the same alteration method across all eighteen licences indicates that they could potentially all belong to a single series, the printing style used on the additional laminate has been identified as a more useful feature, and it is considered unlikely that the same source will use three different printing modes to produce the same product, as this goes against rational choice theory and routine activities theory [145, 146]. With this being the only extractable feature, these linkages are somewhat tenuous, but they do provide some indication as to the potential structure of the forgery market in NSW, with all these documents having

been seized across three different areas of Sydney city. Furthermore, it illustrates the utility of the OVD layer on these documents, with the laminate positioning in relation to the printing making it obvious when the document has been altered.

From examining the rest of the document template and the original date of birth on the document, all these individuals had their date of births altered to appear over eighteen, with the date of birth being the only altered part of the document. Coupled with the fact that these documents were most likely surrendered to police during licencing checks at local establishments that serve alcohol, it appears that the forged photo cards have been used to gain access to alcohol and other restricted services by underage individuals.

2.4.2.4 Quality indexes

The quality of the counterfeit Australian licences was determined by examining the number of security elements and core design features that were correctly replicated by the manufacturer. These features included the security features such as microprinting and OVDs, along with visual features such as logos. A higher percentage quality of the document indicated that more features were correctly replicated. This can provide insight into the document templates and features that are particularly vulnerable to counterfeiting or alteration, and those series that pose a higher risk (i.e. those that are of a higher quality). The number of extractable features varied across the different document templates, with the NSW licences having the most features (6), followed by WA (5) and VIC (3) as no UV images were provided for the VIC licences.

Across the 157 counterfeit Australian licences examined, 135 (86%) of them had a percentage quality of less than 50% (Table 2.12). The average quality index for NSW counterfeit licences

was 25% (68 documents), 33% for VIC counterfeit licences (70 documents) and 77% for the WA counterfeit licences (19 documents).

Table 2.12: Average quality index (%) per series within the counterfeit licences document set. Those series that have an average percentage quality of over 50% have been highlighted, with those that pose the highest risk highlighted in red and orange.

Document Type	Series number	Average quality index (%)
NSW Counterfeit Licences	NSW_DL1	33%
	NSW_DL2	20%
	NSW_DL3	28%
	NSW_DL4	11%
	NSW_DL5	29%
	NSW_DL6	0%
	NSW_DL7	6%
	NSW_DL8	13%
	NSW_DL9	0%
VIC Counterfeit licences	VIC_DL1	33%
	VIC_DL2	36%
WA Counterfeit licences	WA_DL1	80%
	WA_DL2	100%
	WA_DL3	67%
	WA_DL4	40%

In general, there was a low quality amongst the NSW licences (average of 25%), 64 of the 68 had a quality of less than 50%, with most of them sitting at 33%, which was equivalent to only two feature types having a replication score of over two. Beyond having a higher number of security features and design elements, the features within the NSW licences were noticeably more complex, meaning that there were more small features that were not replicated properly and would often go unnoticed by a forger. This increased complexity likely impacted the

overall quality of the documents and therefore made them more difficult to convincingly replicate.

Much like the NSW licences, the VIC documents also had a low average quality (33%), with only one of the 70 documents with a percentage quality over 50%. While the VIC licences only had three extractable security features to determine the percentage quality (due to the lack of UV images) the features in the VIC licences appeared to have a similar level of complexity as those within the NSW licence, particularly in relation to the microprinting, with no manufacturer correctly replicating the legitimate microprinting.

Contrasting with both the NSW and VIC licences, the WA documents had the most documents with a high percentage quality, with 17 of them having above a 50% quality index, and five having successfully replicated all identifiable security features to a high enough standard to likely convince a lay person of their legitimacy (100% quality index). This was undoubtedly due to the lower complexity of the WA licence features. The microprinting for example, was successfully replicated in five of the documents, as it is not small or complex enough to prevent replication.

When examining the percentage quality of the series, as illustrated in Table 2.12, the series that poses the greatest risk, i.e. that which has replicated the most security and design elements, is WA_DL2, as all documents within this series replicated all security features and design elements to a high standard. This may be indicating that changes are required within the WA driver licence to make it more secure, and thus more difficult to convincingly counterfeit. However, if new features are to be integrated into this document type, it is crucial that the complexity of these features is increased. Simply updating the style of a feature (without increasing its complexity) is not a sufficient counterfeiting deterrent, as forgers are known to be highly adaptable [27, 28, 51, 120]. This was illustrated by the WA government's

introduction of a new OVD style into the WA driver licences in 2015. As illustrated in this data set (Figure 2-16), both OVD styles, being those from pre- and post-2015 have been replicated.

(a) Coat of Arms style (from 2001)

(b) State and Kangaroo Paw flower (from 2015)

Figure 2-16: Both versions of the OVD feature introduced onto the WA licences. Style (a) was introduced in 2001 and featured a repeated pattern of the coat of arms of WA (like that on the left of the image). Style (b) was introduced in 2015 and features the state of WA and a Kangaroo Paw, the state's floral emblem.

Furthermore, by examining the proportion of the documents that have replicated specific security features, it is possible to get insight into what features are the most effective for preventing counterfeiting. Table 2.13 shows the different document types, along with the extracted security features of interest and the percentage of documents in which the feature was replicated to a high enough standard that it could be perceived as legitimate. Across all licences, the feature that was correctly replicated most consistently was the optically variable device (OVD). While this OVD feature is useful in preventing and identifying forged documents (i.e. those that have been altered), as illustrated in Section 2.3.2.3, it is not an effective feature for deterring counterfeiting.

Table 2.13: The most vulnerable security features across the documents sets, indicated by the percentage of the document sets that successfully replicated the security features of interest.

	Document type		
Feature	**NSW Licence**	**VIC Licence**	**WA Licence**
Substrate UV	9%	19%	37%
OVD	72%	80%	84%
Logo	12%	-	89%
UV logo	4%	-	84%
Microprinting	0%	0%	89%

Clearly, as indicated in Table 2.13, microprinting is the most effective security feature to deter counterfeiting. However, this is contingent on the microprinting being small and complex enough that it can't be replicated through regular printing methods, as illustrated by the high percentage of documents that successfully replicated the WA microprinting. Interestingly, previous research has indicated that UV features should not be used to authenticate documents, as they are often successfully replicated, with UV security printing of some counterfeit Portuguese ID cards having a quality index of 70% [13]. However, as has been found here, if the UV feature is complex enough, such as the feature within the NSW licences, it can be considered an effective deterrent, and a useful tool for detecting the counterfeit documents.

Increasing the complexity of these security features would also assist the profiling method, creating more characteristics of interest that could be extracted and profiled, making the identification of series and linked documents easier, but also more reliable. It is clear from this analysis that the NSW documents are the most secure documents of the ones analysed in this research, with them exhibiting counterfeits of the lowest quality, and the lowest number of features being properly replicated.

There is of course an intrinsic bias associated with this kind of analysis, as all the documents examined here were of a low enough quality to be detected by law enforcement. It is therefore

even more concerning that the WA licences examined here were of a such a high quality, as these would be, in theory, the lowest quality WA documents in circulation. This illustrates the potential risk that is being posed by these documents.

The analysis of the quality index of features may potentially assist in guiding decisions of those organisations that are routinely authenticating documents, as well as those that are manufacturing the security elements, helping guide them in advancing particular security features of interest, or providing guidance regarding the most efficient way of detecting counterfeits. Based on the analysis here it is advised that examining the microprinting is an effective way to efficiently authenticate NSW, WA and VIC driver licences. However, a closer examination is likely required for most WA licences, given the high-quality indexes identified in this work. Of course, this examination is just a first step, on quite a small scale, but the information provided can still inform front-line workers and security organisations. It also provides an indication of the potential outcomes of this method, illustrating the benefits of implementing a systematic forensic intelligence model for fraudulent identity documents in Australia.

2.5 Algorithm-based comparisons (Padif)

Twenty-six provisional NSW driver licences that were physically examined from Organisation 2 were uploaded into a secure version of ProFID and then compared using the integrated semi-automated comparison algorithm software, known as Padif. The aim of using Padif in this work was to determine if it could be used to compare Australian documents, therefore further illustrating if ProFID/BIDIF could be integrated within Australian policing. While three analyses were conducted using Padif, only the results for Analysis 01 have been included here for illustrative purposes. All ROIs and the respective dendrograms can be found in Appendix Figure A. 2 to Figure A. 5.

All Padif analyses utilised a combination of ROIs including features of interest identified through the manual profiling approach (such as the microprinting, state badge and errors on the back of the card), and areas of template text such as 'Driver' in the red coloured bar and 'Conditions' on the front of the card in Figure 2-17.

(a) (b)

Figure 2-17: Regions of interest for Padif Analysis 01 on the front of the licence (a) and the back of the licence (b)

The results of the Padif analysis are shown in Figure 2-18, with the colours corresponding to the series (NSW_DL1, NSW_DL2, NSW_DL3 and NSW_DL5) that were identified through the manual profiling and comparison process. In almost all analyses conducted, the groups that

Padif identified agreed with those identified through the manual profiling process, although there was some separation occurring between two of the documents from NSW_DL1 and the rest of that series. In every analysis these two documents were identified by Padif as being quite different to the rest of the series, most likely due to the difference in the vibrancy of the printing, particularly in the microprinting (as illustrated in Figure 2-19). Despite this difference in colour, these two documents are part of the NSW_DL1 series as they were linked based on the style of the security features, the errors on the back of the card, and the serial numbers.

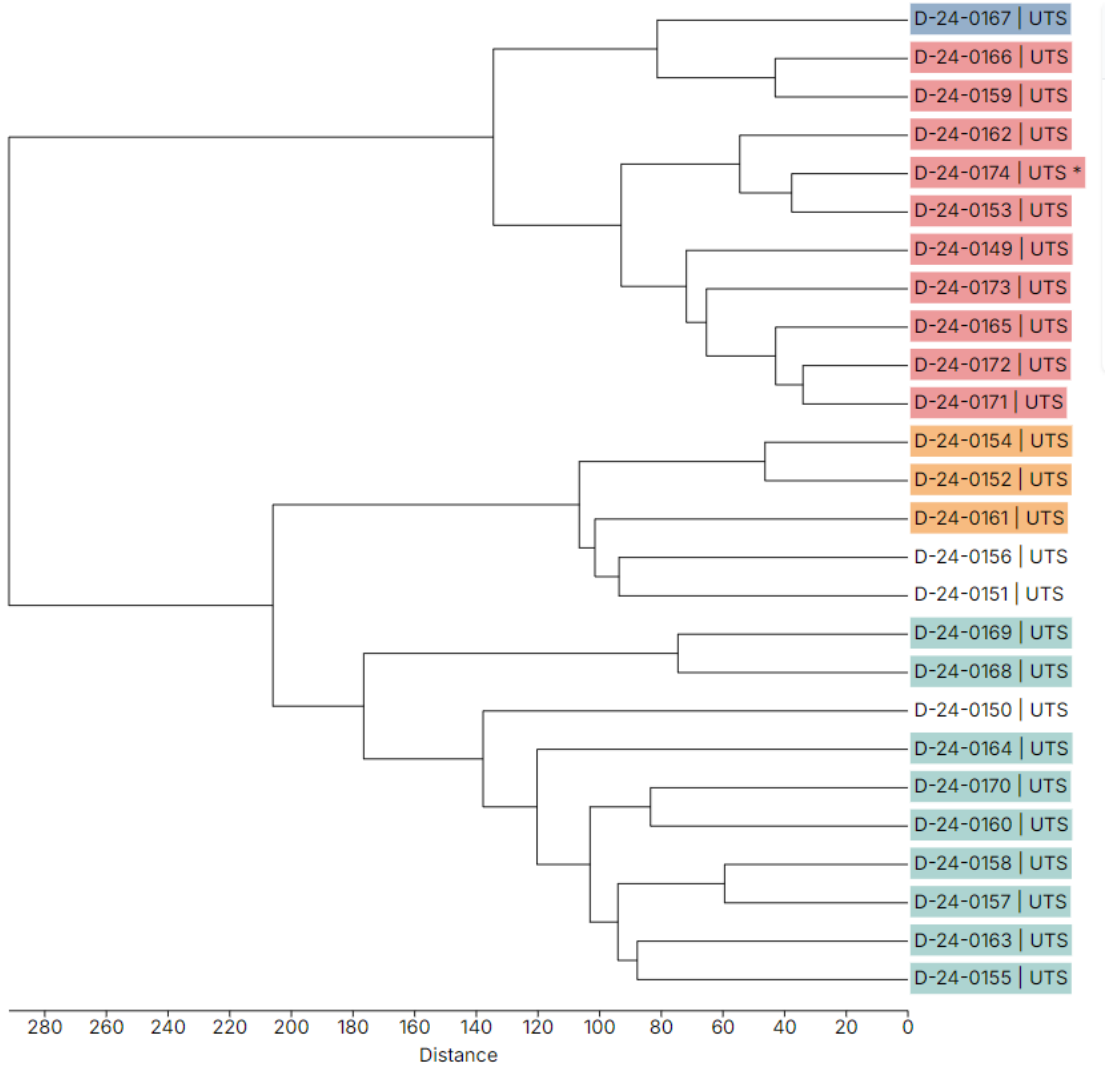


Figure 2-18: Dendrogram results of Padif Analysis 01. Each colour designates the series that the document was identified as belonging to through the manual profiling (NSW_DL1 = pale teal, NSW_DL2 = red, NSW_DL3 = orange, NSW_DL5 = blue).

(a) (b)

Figure 2-19: Differences between the documents within series NSW_DL1. The style of document that Padif separated from the rest of NSW_DL1 (a) along with the style of the rest of the documents within NSW_DL1 (b)

In all analyses, the most consistently grouped series was NSW_DL2. Equally as consistent was the fact that Padif identified document D-24-0167 (which is part of NSW_DL5) as being similar to some documents within NSW_DL2, in particular document D-24-0166. This link was investigated, and it was found that the two documents shared some obvious similarities, the most notable being on the back of the card, including the font, bracket style, address, and mistakes in punctuation. However, there were some errors in D-24-0167 that have been corrected in D-24-0166, including the change in state badge and the correction of 'Tracker' to 'Tractor' as highlighted in Figure 2-20. There is the possibility that, given the similarities between these documents, and the differences, that D-24-0166 (and the rest of NSW_DL2) could be an evolution of D-24-0167 (and therefore the rest of NSW_DL5). Of course, this is impossible to say with certainty without the contextual information of when and where the documents were seized.

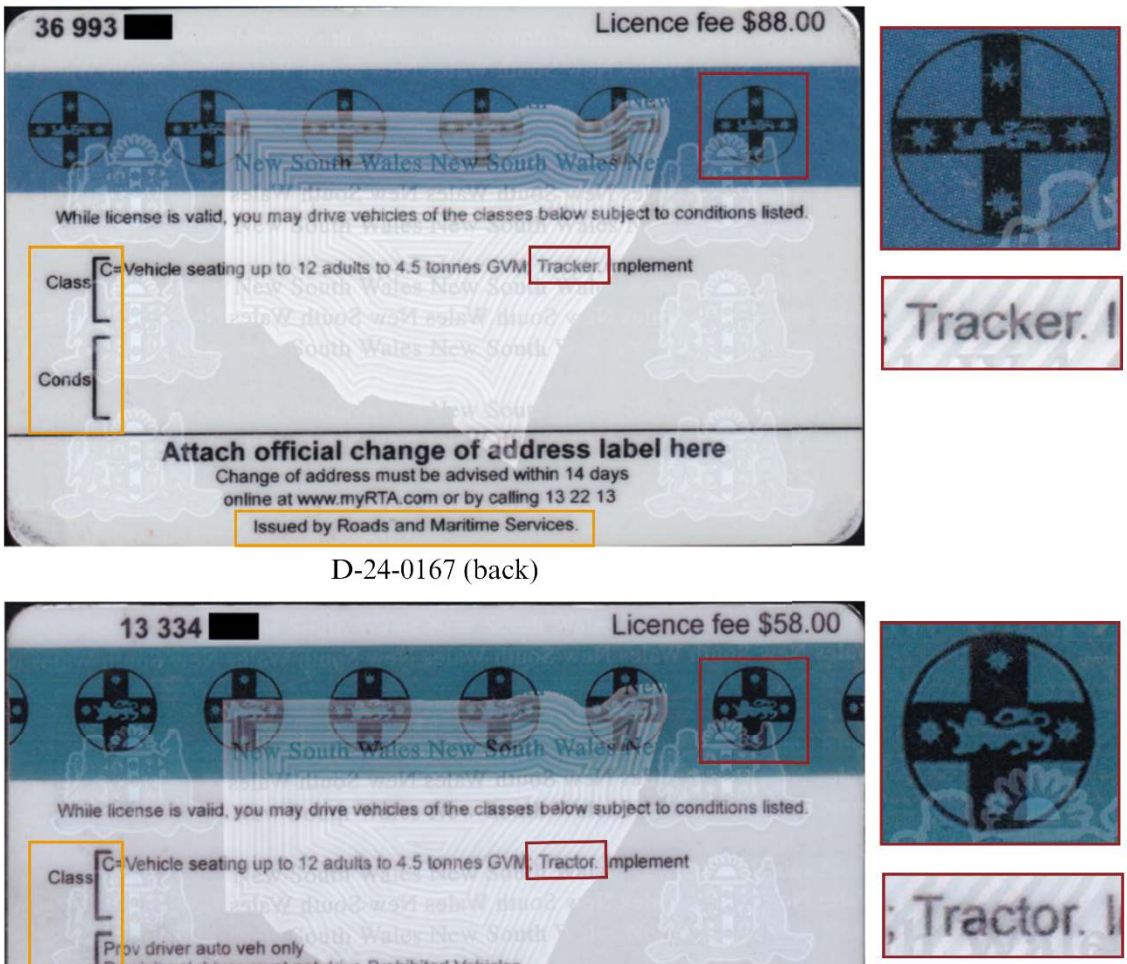
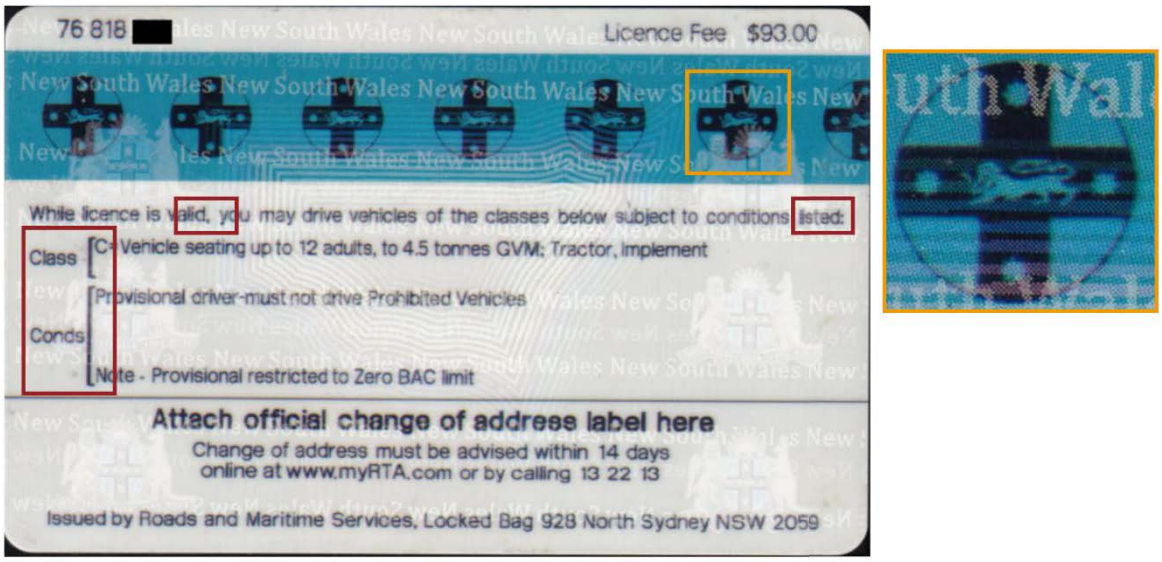


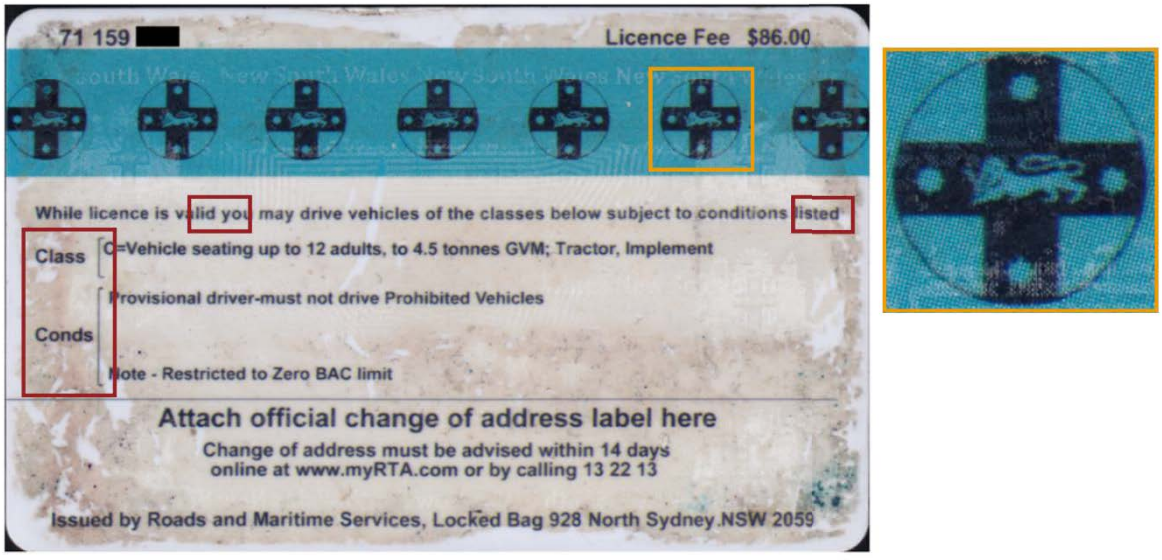
Figure 2-20: The similarities (yellow) and differences (red) between documents D-24-0166 and D-24-0167 that were identified as similar by Padif

The Padif analysis also suggested a potential link that had not been identified within the manual comparisons. Documents D-24-0156 and D-24-0161 (part of NSW_DL3) were identified as being similar in all five of the Padif analyses, and upon further examination of the two documents there were some visual similarities between the documents, most notably, in the security elements that were used, such as the microprinting and the style of the state badge.

However, there were some noted differences between the fonts used on the back of the licences, as well as differences in the positioning and style of some elements (such as the brackets), and differences in punctuation (Figure 2-21). When comparing these documents manually, they were identified to have a 24% similarity and were therefore not considered to be linked.



D-24-0156 (back)



D-24-0161 (back)

Figure 2-21: Comparison of the back of documents D-24-0156 and D-24-0161 which were identified as being linked by Padif. The similarity between the styles of state badge is emphasised (cut outs), however, there are noted differences in the font and punctuation along with the style and placement of some elements such as the brackets, as indicated in red.

Given that the overall templates of these documents share some similarities, there is the possibility that the same document template (including base features such as the state badge) was purchased from the same manufacturer and subsequently edited by two different forgers. As document precursors (e.g. substrates, inks, and security features) have previously been intercepted in the post [51], this could explain the similarities in core visual security features (e.g. the microprinting and state badge) and colouring of design elements, with the difference in fonts being introduced by the editing of the template. This is of course, just a hypothesis.

Overall, this is a good illustration of how the semi-automated algorithms of Padif pick up on different qualities within the document compared to the manual method. When used in partnership with the manual profiling method, also referred to as the human approach, the use of these algorithms can assist in identifying or suggesting potential links that the examiner may have missed, which can be especially helpful when dealing with large document sets. In this way, Padif can assist the document examiner as a triaging tool to more efficiently process large document sets (with it taking less than seven minutes to process 26 documents with six ROIs) and as a confirmatory tool as it was used here. In comparison to the manual method, which can take between 5-10 minutes per document depending on the number of features being extracted, the use of Padif can significantly speed up this process.

Clearly, from this analysis, the semi-automated algorithms embedded within the ProFID and BIDIF systems effectively compared the provisional Australian driver licences. While the presence of OVDs across the entirety of the front and rear surfaces of the documents was initially cause for concern, and made the selection of ROIs somewhat difficult, Padif still performed well. The algorithms were able to identify the document series correctly (based on the manual method) and even assisted in the identification of other potential links and documents of interest to look at more closely. There were some erroneous identifications of links between documents that were visually dissimilar, however, these erroneous linkages were

quickly identified as such, so did not negatively impact the overall results, or the efficiency of the method. However, Padif cannot be used in isolation, rather a complementary method combining the human, subjective manual method, with the semi-automated method of Padif is required [51]. Whether being used as a triaging tool or as a confirmatory method, the human analyst's expertise will always be required, not only to ensure that the machine is performing appropriately, but as the interpretation of the links, their value and overall meaning cannot be determined by Padif in isolation. The efficacy of Padif on the documents examined here is another clear illustration of some of the benefits of implementing a systematic profiling method for fraudulent documents, such as ProFID/BIDIF in Australia.

2.6 General discussion and conclusions

To provide some insight into the Australian criminal environment for document fraud, 183 fraudulent identity documents seized from three different Australian policing and security organisations were examined, visually profiled, and then compared. Of the 183 documents within the data set, 94% of them were linked to at least one other document, and 17 series emerged. 26 of these documents were also then compared using the semi-automated comparison algorithms housed within ProFID, known as Padif. Not only did Padif function well as a confirmatory tool, identifying all the series that were manually highlighted, but it also helped to spot potential document evolutions and links that were not detected during the manual process.

The results presented in this chapter suggest that the profiling method, both the automated and manual versions are not only effective on Australian driver licences but may help identify the structure and organisation of the fraudulent document market. It may also assist in the identification of prolific offenders and as illustrated here, can assist in the identification of cross-jurisdictional, and/or cross-organisational links. So far, the general attitude towards document fraud has been very reactive, with the general misconception being that fraudulent documents are just tools for under-age individuals to gain access to restricted services. Of the documents examined in this work, 94% of them were linked to at least one other document, and the largest of the fifteen series identified was made up of 54 documents, highlighting that there may be prolific offenders operating within the Australian market, and that the overall market is likely to be organised. Of course, at this stage, this is just a proof of concept, but the results here are a promising first glance at the potential of this method.

The utility of the visual profiling of fraudulent documents goes beyond the identification of linked documents and therefore the structure of the market. The close examination of the

security features and design elements that are successfully replicated by manufacturers can provide information about the document types that are at the most risk of being counterfeited, and that therefore pose a greater threat (i.e. are more likely to fool authenticators). The intelligence provided from these examinations can assist on the front lines of document authentication but can also assist decision makers and document manufacturers in identifying security features that need to be improved, or document templates that need to be updated, thus proactively working to help reduce the document fraud criminal environment.

Of course, in this kind of work it is impossible to say with certainty whether those documents that are identified as being linked are, without a doubt, originating from the same source, aside from those that are physically seized from the same location or factory. This is especially true within the document set examined in this research due to the lack of contextual information that was gathered when they were originally collected. While it is impossible to get to the ground truth of where these documents have come from, some steps have been taken to try and minimise this level of uncertainty as much as possible. Targeting features that are intrinsically related to the choices that the source must make during the manufacturing process as well as using a multi-feature approach ensures that there are very few possible hypotheses to explain a link, other than the documents having originated from the same source [15, 16, 144]. This is one of many benefits of relying upon a multi-source approach; by focussing on a combination of features as opposed to a single feature to establish links, it provides more weight to the linkages and enables the identification and assessment of evolutions in the features and methods used to manufacture the documents.

Even so, there is an unavoidable element of uncertainty in this work, like in the analysis and interpretation of any trace [194], and while the use of these links and this profiling method still fits well within the accepted levels of uncertainty of forensic intelligence [16], it must be kept

in mind that these results only represent a model of the criminal environment, and are not a flawless depiction of reality [195].

Of course, while keeping these potential uncertainties in mind, the value that can be gained from this method is clear, particularly in its ability to provide insight into the criminal environments of not only document fraud but also organised crime and terrorism, as illustrated internationally. So far, the ProFID system has been successfully integrated across 14 European countries, and a total of 11,159 fraudulent identity documents have been integrated[16]. Of these documents 25.45% of them have been linked to at least one other document, and nearly 500 series have been identified. Focussing specifically on domestic links, Switzerland has integrated 3,714 documents, with 40.5% of them identified as being linked [163]. The presence of international, cross-jurisdictional links that have been identified using ProFID [143], along with the organised crime networks that have been identified and subsequently dismantled [37], clearly illustrates the benefits of implementing such a system. While the research in this chapter indicates that the Australian fraudulent document market is likely organised and would therefore benefit from the implementation of a system such as ProFID, it is a natural next question to wonder whether the level of success attained in Europe could also be achieved in Australia.

Understandably it is hypothesised that there would be some differences between the document fraud criminal environment in Europe, and that of Australia, not only due to differences in policing, but also perhaps due to the very different geographical climates of each country. However, when comparing the organised crime environment of Australia with that of Switzerland (the country with the highest contribution of documents to ProFID), the types of criminal groups that are operating in each of these countries are quite similar. In both regions

[16] As at 06/02/2024

there are organised crime networks including international mafias as well as OMCG's [186, 196], with the main difference being the origin country of these different groups.

According to the Global Organised Crime Index (GOCI), compared to Switzerland, Australia has a slightly higher presence of criminal networks, extortion, and protection racketeering, linked to the prevalence of OMCG's in Australia. Additionally Australia has a higher prevalence of flora and fauna crimes, as well as the trade of heroin, cocaine, and synthetic drugs, among a few others [186, 196]. The difference in geographical position of Switzerland, being that it is landlocked by five countries, along with its location in Europe means that the Swiss criminal market is largely controlled by foreign actors such as Italian mafia groups, Balkan mafias, and West African gangs [196]. This positioning undoubtedly contributes to the sheer number of international fraudulent documents that are encountered by police and subsequently processed within ProFID, with counterfeit Italian ID cards being the most prevalent document in the system. Unsurprisingly, the most entered documents for almost all countries contributing to ProFID have been those from other European countries.

Obviously, the geographical positioning of Australia is drastically different to that of Switzerland, with it being waterlocked and in closer proximity to New Zealand, Papua New Guinea, Indonesia, and greater Asia. The obvious result of this is that there is a far higher participation of organised crime groups from these regions within Australia [186, 190, 191]. Furthermore, drugs entering Australia are largely originating from South East Asia, with international syndicates linked to Hong Kong, Southern China, and Malaysia [186]. The most prevalent criminal groups within Australia are OMCG's, with them taking part in a broad range of illegal activities that are facilitated by significant connections with traditional organised crime groups [168, 186]. In combination with these OMCG's other traditional organised crime groups have been present within Australia including Italy's Ndrangheta group as well as organised crime groups of Southwest Asian and North African origin among others [47, 167,

168, 183-186, 188-192]. Overall, according to Interpol, approximately 70% of serious organised crime that is impacting Australia either originates internationally or at the very least has strong offshore links [197].

In both Australia and Switzerland, there is a high rate of international organised crime involvement in domestic activities. This suggests, in combination with the research conducted in this thesis, that the ProFID/BIDIF system would be a valuable addition to Australia's fight against serious organised crime, both internationally and domestically. The implementation of ProFID in Switzerland has shown promising results, and the geographical positioning of Australia could assist in filling a significant gap in the current implementation of ProFID being the Asia-Pacific side of the fraudulent document market, with the majority of the documents currently within the ProFID system being of European origin [163].

While it is hypothesised that the integration of ProFID within the Oceanic region and Asia would assist in the identification of links between documents seized throughout these regions, there is also the possibility of identifying links between Australia and Europe. Admittedly, Australian documents are not often encountered in Europe, with less than five Australian documents currently within ProFID [163]. However, a link was identified between a driver licence from Great Britain seized in Australia by NSWPF and one intercepted in Geneva, Switzerland. This link was identified when, as a trial, the four international documents seized within Australia were compared, using both the manual profiling method and Padif, against those of the same type seized throughout Europe. This emphasises the fact that if the method was expanded to include not just Australian driver licences, but both Australian and international passports and other international documents that are encountered by Australian police and border control, this could potentially result in the identification of more links between Europe and Australia.

A systematic forensic profiling system for fraudulent documents such as ProFID would facilitate increased information sharing, not just between domestic organisations, which is required to properly understand the domestic document fraud criminal environment, but also information sharing on an international scale. This is crucial when considering the transnational nature of identity crime and document fraud along with other serious, organised crime. By targeting the fraudulent documents of individuals and comparing them to other international document seizures it would be possible to identify targets or persons of interest before they officially enter the country. Based on the documents within ProFID and trends in series that are identified, 'alerts' are sent to communicate these trends to front-line document examiners such as border security and police, enabling them to identity potential threats on entry to the country, or through routine police operations or other identity checks. This international intelligence network would enable easy communication between jurisdictions and countries to help reduce linkage blindness, increase public safety and reduce, prevent, and disrupt organised crime and terrorist networks.

Currently, in Australia the degree of communication between organisations in relation to fraudulent identity documents is lacking, as illustrated through the cross-organisational links identified within the NSW_DL1 series. According to the manual profiling method, the documents within the NSW_DL1 series, that were seized by two different police and security organisations within Australia have been created by the same source, but prior to this comparison process they were not identified as being linked. Of course there is some communication occurring between these different organisations, as well as collaboration at different levels, but the lack of priority given to fraudulent identity documents across the board, in combination with the general unwillingness to share information across different organisations [198] means that significant intelligence is being regularly overlooked. In general, this attitude towards fraudulent identity documents has led to them being sidelined as

traces and simply being stored in relation to other cases, kept for training purposes or destroyed with no record keeping. This attitude needs to change first and foremost before any systematic intelligence method can be implemented.

This research has illustrated that the systematic intelligence model that has been implemented within Europe would work within the Australian criminal environment and on Australian documents, however, that isn't to say that the system could be immediately implemented. Some significant changes would be required within Australian security and policing organisations to ensure that the full potential of the system was accessed. To further this examination, changes need to be made in the current processes used by policing organisations when collecting and handling fraudulent documents as exhibit types. Not only does contextual information need to be more routinely gathered and made available for such analyses, but documents that are gathered through processes external to investigations, e.g. licensing checks, should still be collected as exhibits, so that the date and location of their collection can be recorded. At a bare minimum this could involve all documents collected during a particular licencing check being treated as a single exhibit, with the date and location of collection officially recorded. This collection of spatial and temporal information could help provide an understanding of where these documents are emerging and when. This could help in the identification of hot spots, or trends in the distribution from manufacturers, which would enable the interpretation of the series level, which holds great potential intelligence value.

Previous research has illustrated that the examination of links and classes at the series level could lead to the extension or commencement of an investigation, the joining of investigations, thus reducing workforce requirements and resources while increasing efficiency, or the confirmation of hypotheses, potentially strengthening a case against individuals or a group of criminals [15]. However, the ability to conduct such evaluations is hampered by the current

attitudes of security and policing organisations to fraudulent identity document collection, examination and storage. While some security and policing organisations in Australia do have some form of routine procedure in place for the photography and then storage of images of the documents, this is not consistent across organisations. If there is to be any hope of implementing or at least working towards the implementation of a system such as ProFID/BIDIF in Australia, there needs to be more consistent, nationwide processes relating to the collection, examination, and storage of fraudulent documents. Something as simple as scanning the documents when they are received using the scanning canvas developed by UNIL, would not only ensure consistent imaging and storage of the document images but would also act as preparation for the implementation of ProFID/BIDIF. This could provide useful intelligence, as capturing documents across a broad range of time and physical locations can provide crucial insight into the fraudulent document criminal environment, something that, thus far, has not been done in Australia.

2.6.1 Implementation of ProFID/BIDIF in Australia

The implementation of BIDIF within Australia will of course be a gradual process, but as an initial starting point a pilot program could be run in one responsive agency such as the NSWPF, or another government organisation that comes into regular contact with fraudulent documents. This organisation would start with an initial ~6-month preparation process (as illustrated in Figure 2-22) with the aim of ensuring the document collection, scanning and upload procedures were standardised across the whole of the organisation which could be facilitated through the distribution of basic training videos. After the completion of the preparation stage, the organisation would move into the pilot study stage. The duration of the pilot study could be dictated by the organisation but given the number of documents gathered across the duration of this thesis, three years is estimated to be enough time to facilitate the collection of enough documents, without taking too long before operational results are generated.

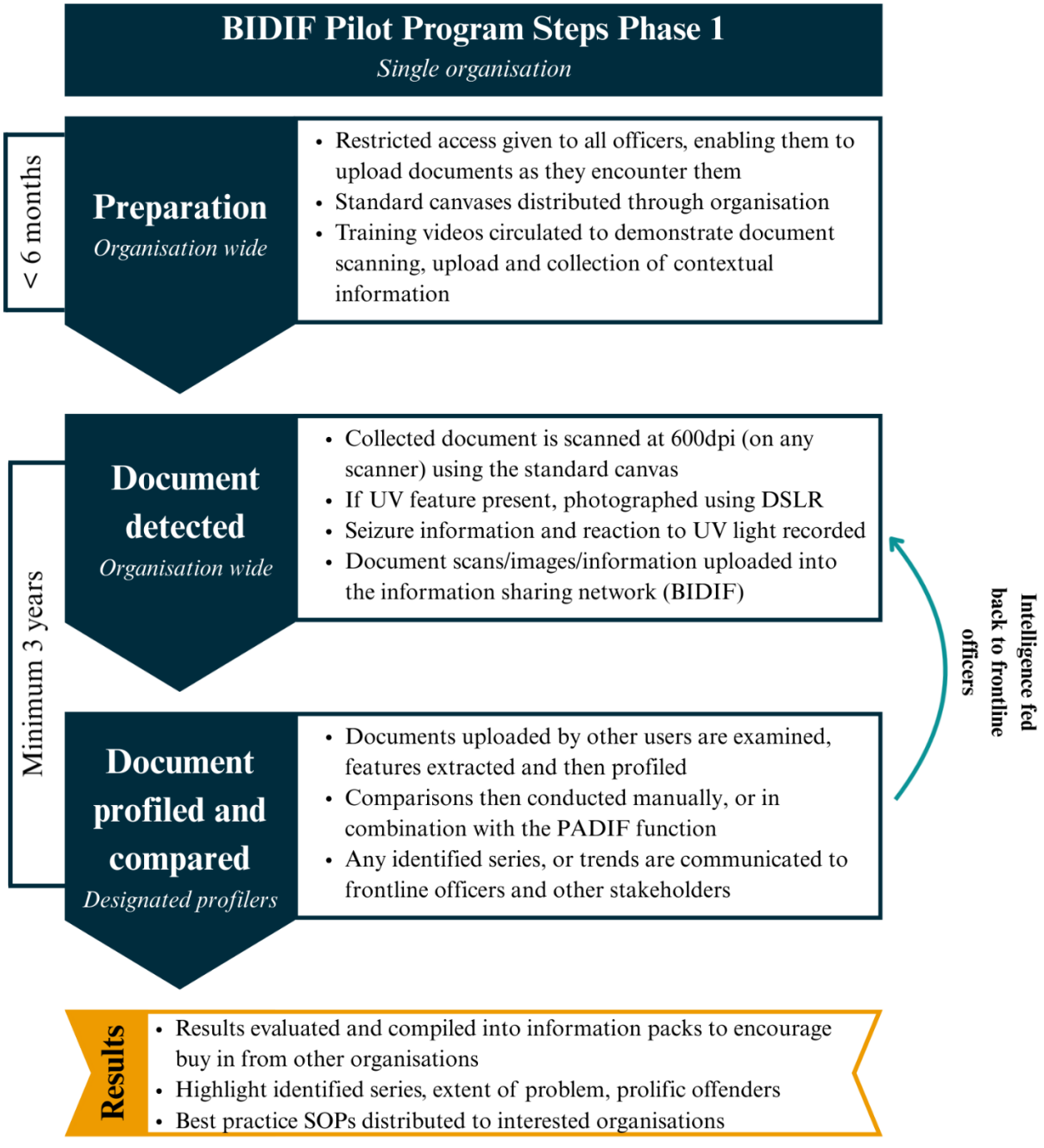


Figure 2-22: The suggested steps of the first phase of the BIDIF pilot program, being the single organisation implementation. These steps can then be repeated as new organisations join the program.

This trial program would replicate the methods used in this research, targeting the identified features of interest, and establishing a standard collection procedure for the fraudulent documents (including imaging and the collection of contextual information). During this pilot study, all officers within the NSWPF would have access to upload documents to BIDIF, so that they could upload them as they are encountered. A designated team, perhaps within the document examination group, would then be responsible for the systematic characteristic extraction, profiling and comparison of the documents. This could be done manually or in combination with the automated comparison process integrated within BIDIF (PADIF). Any identified trends or series would then be communicated to other frontline officers, or stakeholders, facilitating the identification of persons of interest, criminal networks, prolific offenders within the document fraud space, as well as trends in the manufacture and distribution of these documents.

The focus here would be to demonstrate the success of the method in case work. At the end of the 3.5 years, or at other time points dictated by the organisation, education packages outlining the success of the method and a best practice SOP could be disseminated to other relevant agencies through the National Institute of Forensic Science Australian and New Zealand Forensic Executive Committee (NIFS ANZEC). This approach would have two-fold benefits, the first being the standardised collection of fraudulent documents over time, both for their profiling and analysis, but also in preparation for the implementation of BIDIF, and second, the case work outcomes of this pilot program could provide clear examples of the benefits of document profiling and assist in getting other organisations on board. This pilot program could run on an iterative basis, with results being periodically released to encourage the buy in of other agencies and organisations as illustrated in Figure 2-23. The following phases of the pilot program would follow the same steps as indicated in Phase 1, but with more organisations

involved. As new organisations are added to the program, the steps would repeat, adjusting the durations of the different steps according to the organisation's needs. Depending on the results of the pilot program, and the organisations involved, this could culminate in the addition of Australia to the international BIDIF network, facilitating international comparisons between documents, and perhaps enabling the identification of international links. Australia would also then become privy to the intelligence alerts generated through BIDIF, facilitating earlier identification of potential threats, and persons of interest that may be operating in, or trying to enter Australia.

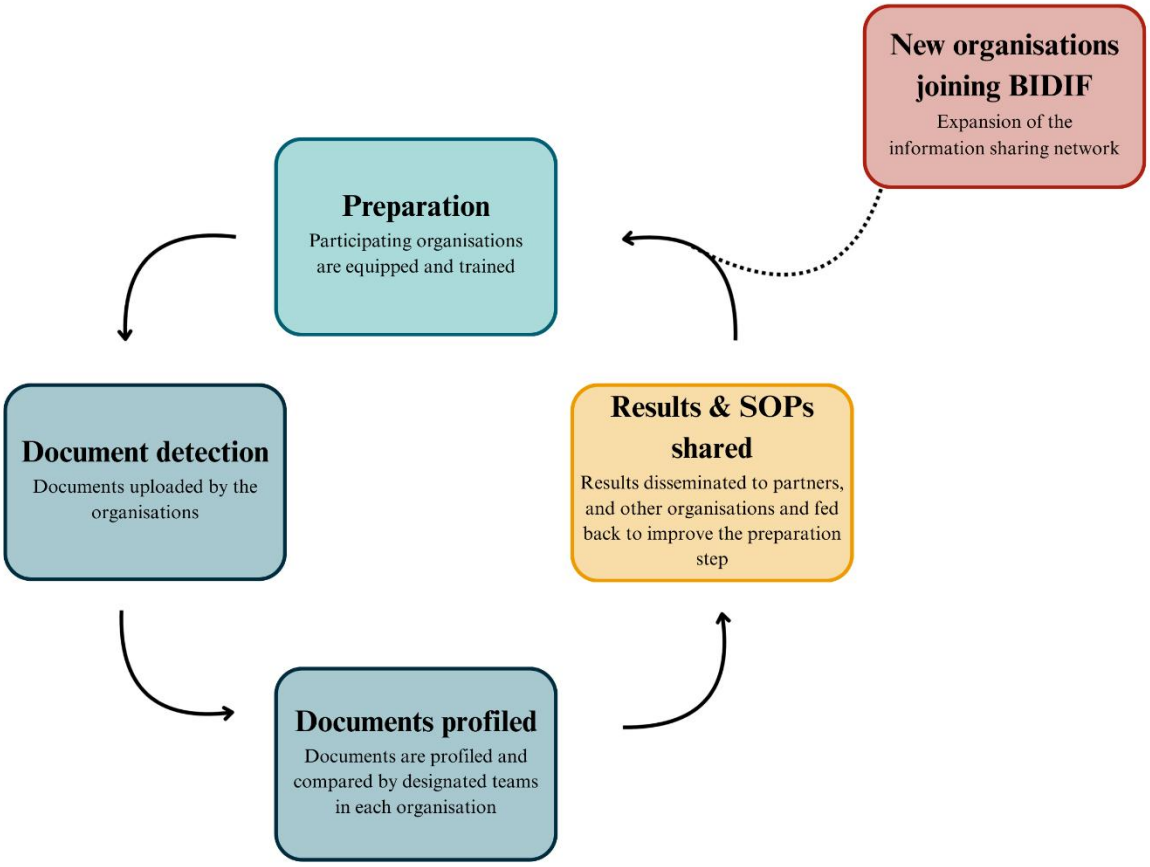


Figure 2-23: The cyclical phases of the suggested BIDIF implementation process to increase organisation buy in.

Chapter

The Investigation of the Online Australian Document Market

3 The investigation of the online Australian document market

3.1 Introduction

Increases in the reliance of society on digital technologies have resulted in an abundance of personal identification information being stored, used, and made available through online avenues. Every time an individual logs into a government website, posts on social media, or fills out an online rental application, they are depositing their information into the web. This, in combination with other advances in technology, has resulted in a digital ecosystem in which identity crime has been flourishing.

A crucial part of the criminal environment of identity crime is the manufacture and distribution of fraudulent identity documents. So far, most research into the document fraud side of this criminal market has focussed on examining the physical environment of identity fraud through the analysis of visual characteristics of fraudulent identity documents (seizures) as illustrated in Chapter 2. However, this research is focussing solely on the physical traces within the fraudulent document market, and when considering that only documents of generally low quality are being detected, this illustrates that the profiling research is only focusing on a fraction of the overall criminal environment for both document fraud and identity crime. While this research is crucial in helping to improve the understanding of the physical fraudulent document market, this approach is only providing a part of the overall picture.

Previous research has illustrated that there is an online trade for fraudulent documents and personal information [199-202], illustrating that examining this online side of the market can provide insight into this often neglected portion of the criminal environment, highlighting key vendors, trends in supply and demand as well as the trafficking of goods. While there are multiple different types of shop fronts and vendors within the online fraudulent document and

personal information market [199, 200], anonymous online marketplaces (a.k.a cryptomarkets) have separated themselves as a particular point of interest, illustrating their intelligence potential in the research of the illicit drug marketplace [96, 104, 117, 203]. While some research has touched on the use of these marketplaces as vectors of information regarding the document fraud criminal environment, most studies have provided overviews of the marketplace [201, 202], rather than conducting an in-depth analysis like what has been done within the illicit drug market, with no research examining the online document market from an Australian perspective.

As illustrated in Chapters 1 and 2, the criminal environments of identity crime and document fraud are complex and multi-faceted. To properly understand these environments, crime traces need to be fully exploited and combined with alternative information from a multitude of sources to ensure the most complete picture of the criminal environment is attained. This research aims to build on previous research into the online fraudulent identity document environment to assist in the creation of a more holistic view of this illicit market and to also illustrate the Australian criminal environment in a way that has, so far, not been done. It is hypothesised that cryptomarkets can provide insight into the criminal environment for document fraud and can facilitate the analysis of the market from an Australian perspective. Furthermore, this information can be complementary to more tangible efforts to understand the criminal environment, such as the forensic profiling of visual characteristics, along with research into the broader identity crime criminal environment. In combination, these two different avenues of forensic intelligence can be used to assist in illuminating a previously shrouded area of the criminal ecosystem.

In this chapter, the focus will be on understanding the cryptomarket-facilitated portion of the online market, and how analyses of these marketplaces can provide crucial intelligence about the criminal environment of document fraud and identity crime. The background information

and theory behind cryptomarkets and their analyses will first be introduced, before providing an overview of the overall illicit market. A more in-depth analysis of the cryptomarket-facilitated trade of fraudulent identity documents and personal information will then be conducted, followed by an examination and discussion of the market for Australian documents.

3.1.1 Dark web basics

3.1.1.1 The internet and its levels

Colloquially, the internet and the web are terms that are often used interchangeably; however, they are two entities that while related, are quite distinct. The internet is a massive collection of computer networks that connects millions of computers globally, enabling and facilitating their communication. The web (a.k.a World Wide Web), is an information-sharing model built on top of the internet that uses the Hypertext Transfer Protocol (HTTP) to transmit data [204]. The web takes up a large portion of the internet and consists of several different layers of accessibility known as the surface (a.k.a clear or open) web, the deep web and the dark web [204].

The surface web is the portion of the web that is readily available to the public, where most day-to-day data and services can be accessed. The information within the surface web is indexed, and much like the index in a book, indexing on the internet refers to the process used by search engines to create lists of accessible information on web pages to facilitate their bulk searching [205]. This is also the section of the web that is under constant surveillance by international governments [204].

The deep web has been speculated to contain around 90% of all the available information on the web [205]. While accessing the deep web does not require any specialised software, the content housed within it cannot be accessed simply through the use of a search engine [206]. It is where confidential files or information can be found, with access often only granted with

specific authorisation through avenues such as personalised login details and paywalls [204, 205]. As an example, most companies such as Netflix, Facebook, and news outlets such as The New York Times (TNYT) have a small portion of their online content available on the surface web, such as teaser articles, or pages including subscription information and costs. All the other pages that are behind their log ins or pay wall are located in the deep web [205].

Often, an iceberg has been used as an analogy to describe the different levels of the web. The deep web correlates to the entirety of the submerged portion with the dark web inhabiting its very tip (as illustrated in Figure 3-1). The main distinction between the deep web and the dark web, is that while the deep web content is protected by log ins and paywalls, the dark web is hidden by design. To access the dark web, one must use specialised networks such as Tor, Freenet or the Invisible Internet Project (i2P) [207]. These different networks are explained in Appendix Table A. 8, except for Tor which is explained below.

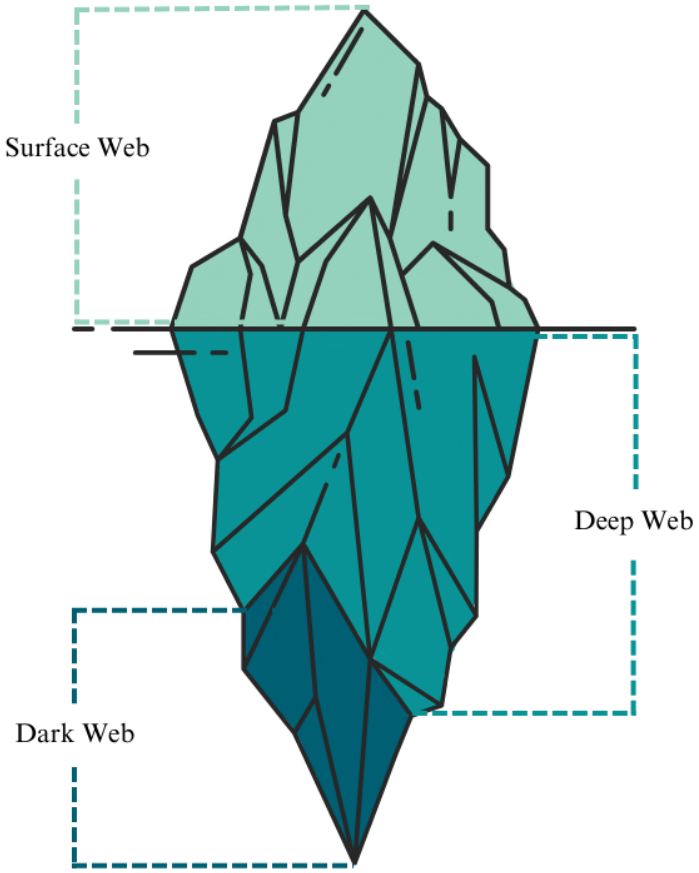


Figure 3-1: The different levels of the web illustrated as an iceberg. It should be noted that this is not to scale but is an analogy to illustrate that what is visible above the waterline (surface web) is only a small fraction of the web, with most of the content being found in the deep web. Adapted from Bedi et al. 2020 [208].

Tor is the most popular and well-known dark web network, which was born out of the onion routing project developed in the 1990s to provide safe communications between whistleblowers, operatives, and covert government agents [204, 209, 210]. Named for its unique way of adding layers to an individual's internet traffic (much like the layers of an onion), Tor keeps the internet traffic of a user private and secure, disguising both their origin and destination [205]. While originally designed for use in covert government operations and communications, in 2002 it was released to the general public [204].

It wasn't long after its release to the public that Tor began to be used by the criminal element, taking advantage of the anonymity it provided to assist in a broad range of criminal behaviours and secret communications [206]. One of these behaviours was the sale and distribution of illicit goods, such as drugs, with Silk Road being one of the first illicit online markets to take advantage of the anonymity afforded by Tor's structure [206].

3.1.2 Silk Road and beyond

3.1.2.1 The journey to Silk Road

While the online sale of illicit drugs can be traced back to the 1960s [211], most sales for illicit goods that pre-dated the launch of Silk Road were carried out overwhelmingly on the surface web, using single actor web shops, or web forums like Farmer's Market which operated on the web from 2006 to 2012 [205, 206]. However, the emergence of the Tor network, in combination with the creation of the PGP (Pretty Good Privacy) protocol for the encryption of messages, files, and documents [212] and the gradual emergence of digital and anonymous currencies, led to the creation of the revolutionary marketplace, Silk Road [206, 213].

While Silk Road took advantage of the pre-existing online drug trade and anonymising technologies (as its administrator Dread Pirate Roberts stated, the pieces were already there [213]) it was the first dark web marketplace that combined the anonymisation and encryption technologies, escrow, dispute resolution and the overall design of the platform economy [206]. This new format gave users an experience that combined the features of the shop and forum formats, providing individual sellers with a storefront from which to operate their business while also having the forum benefits including dispute resolution and enforced rules [206]. The benefit of the implementation of the escrow system was also clear, with administrators acting as mediators through which all funds move [214]. In this system, once an item is purchased, the funds from the buyer are held by the administrators until the transaction is marked as finalised or the item is marked as delivered by the buyer [214]. Replicating some portions of

licit online stores such as eBay and Amazon, Silk Road was a platform that buyers and sellers were able to use to facilitate transactions in return for a commission on the sale, with administrators providing governance and organisation [214-216]. The replication of these institutional safeguards, along with the organisational structure and appearance of Silk Road is something that has been replicated in all cryptomarkets that have been opened since, earning Silk Road the descriptor of being a "paradigm-shifting" illicit online economy [206, 217].

During its years of operation (2011-2013), Silk Road was the apex of the online drug trade, facilitating an estimated $1.2 billion in transactions [205], with it often being credited as causing the increase in the demand for illicit drugs through the dark web and the increase in vendors. So much so, that its success led to the creation of numerous copycat marketplaces [206]. Even today, over a decade after Silk Roads' initial launch, its cryptomarket 'formula' is still being followed, mimicking its platform design, technologies for anonymisation, encryption and the use of escrow and dispute resolution services [206].

3.1.2.2 The time after Silk Road

After Silk Road's closure in 2013, the cryptomarket environment was characterised by a state of flux, with numerous markets emerging in an attempt to fill the vacuum created by the FBI's identification and arrest of the market's administrator Ross Ulbricht, a.k.a Dread Pirate Roberts [206]. Users began to flock to the smaller competitor markets such as Sheep Marketplace and Black Market Reloaded, which both experienced massive growth following the fall of Silk Road [206], along with Agora, Silk Road 2.0 and Evolution Marketplace [206]. In general, most cryptomarket trade will be concentrated on the 'top tier' or 'apex' markets, of which there are usually between one and four (except in the aftermath of a closure) [206, 218], with a handful of smaller markets existing around them. The concentration of activity, known as centralisation, was first noticed after the closure of Silk Road and was further highlighted by Operation Onymous in 2014 [206, 219], with it now considered to be a repeating pattern that

is characteristic of the cryptomarket ecosystem [218, 220, 221]. As one market closes, buyers and vendors will migrate to competing markets [218, 220, 221], with them often operating backup profiles on smaller marketplaces [218].

In particular, cryptomarkets became alternative avenues to purchase drugs, with cryptomarket-facilitated drug sales being most prominent in the regions where cryptomarket use is the highest, being countries within Europe, North America, and Oceania [106, 107, 222, 223]. Overall, cryptomarkets are considered an attractive alternative to in person sales for both buyers and vendors due to the many advantages, including cheaper prices, likely due to increased competition between vendors, access to greater variety, higher purity (or at least perceived purity) [224, 225] and reduced risk of physical violence [206]. Undoubtedly, the anonymity associated with the use of cryptomarkets and some cryptocurrency, is also an added advantage that has driven both buyers and sellers to utilise these online economies [206].

While the criminal behaviours typical of the cryptomarket environment (such as centralisation) would, in theory, make these marketplaces highly susceptible to law enforcement action, for the most part, the overall cryptomarket criminal environment is resilient. Undoubtedly because of the sheer number of cryptomarkets in operation at any one time, most law enforcement actions simply result in the displacement of illicit activities [206, 220, 221, 226, 227].

3.1.3 Cryptomarket life cycle

While the overall cryptomarket criminal environment is resilient, the individual markets themselves are significantly more vulnerable, with most of them only operating for a short time before their closure. In 2017, a review of 87 cryptomarkets found that more than 80% of the markets were shut down within their first year of operation, with an estimated 60% remaining active for less than six months [228]. The degree of vulnerability of a cryptomarket is largely

dictated by its time active and its size (number of buyers and vendors) as summarised in Table 3.1 [206].

Table 3.1: Summary of the different stages of a cryptomarkets lifecycle adapted from Martin et al. 2019 [206]

Life stage	**Characteristics**
Infancy	< 6 months active Initial launch and marketing activity
Adolescence	6-8 months active Modest growth and developing stability in the marketplace Vendors with profiles on more mature sites may begin creating backup profiles on the adolescent sites
Maturity	18+ months Greatest potential reached in terms of overall size and profitability
Death	Market taken offline due to exit scam, voluntary exit, external hacks or being taken down by law enforcement

The most likely cause of cryptomarket death is through an exit scam, being the theft of all escrow funds by administrators, with 45% of cryptomarket closures being attributed to this cause [109, 228]. Another 30% of the closures can be attributed to the voluntary exit of the market from the ecosystem, in which the administrators forewarn the vendors and buyers of the closure of the site, enabling them to set up profiles on other markets, and remove their funds [109, 228]. Coming in third regarding degree of likelihood, is the market being hacked by an external party, often with the theft of private information or cryptocurrencies being a main motivator [109, 228].

The last cause of death, and the most interesting for this research is death by law enforcement take down. This is the least likely cause of death among cryptomarkets, with only 15% of

deaths being attributed to this cause, often being the larger, more mature markets [109, 228]. However, it has been identified that individual closures of marketplaces have very little impact on the overall criminal environment, largely due to the vendors and buyers displacing their activities to other markets [206, 220, 221, 226, 227]. While law enforcement activities do help to keep the more mature markets in check, preventing them from becoming an untameable force (as was illustrated by Hydra when it was left unchecked by authorities [229]), the overall strength of these often-reactive investigative tools used by law enforcement are arguably quite limited in their current form [206, 220, 226].

3.1.4 Limitations of law enforcement crackdowns on illicit marketplaces

Much like the traditional case by case approach typical of reactive policing, most law enforcement operations have focused on police crackdowns of cryptomarkets, concentrating on the largest markets with the widest reach. In most cases, these operations are accompanied by a public relations and media campaign to publicise the police actions [220]. In the past, police crackdowns have been one of the most popular methods to attempt to deal with illicit markets, especially the physical markets for illicit drugs [220]. However, there is little evidence that this tactic has been effective in reducing the supply and demand of illicit goods and services [220, 230-233]. Most studies found that there was a negligible impact on the criminal environment for illicit drugs, with no impact on the number of drug users or suppliers, the prices of drugs or the number of individuals entering treatment centres [227, 231, 233, 234].

Despite this lack of impact on the physical market, with the emergence of Silk Road in 2011, law enforcement was quick to adopt these practices to attempt to combat these online marketplaces. Admittedly, law enforcement takedowns have been successful in shutting down some of the most popular cryptomarkets. However, when examining it from a bigger picture lens, the tangible impacts of these crackdowns on the overall criminal environment is hard to

estimate and appears to only really impact the criminal environment on a smaller scale. Only a small proportion of market deaths are due to law enforcement action (15%) [109, 228], and most actions simply result in the displacement of the criminal activities [220, 226, 235, 236]. As was observed in the physical market for illicit drugs [227, 232, 233], these law enforcement actions have limited, short-term impacts on the cryptomarket environment [206, 220, 226, 237]. Some have even argued that these law enforcement operations may be stimulating the cryptomarket criminal environment through the free publicity generated by the media attention [235, 237-239], as well as technological innovations prompted by market closures and security breaches [235, 238, 239].

This indicates that police interventions and crackdowns, while temporarily stalling the activities within the cryptomarket ecosystem, don't have much long-term impact on the overall criminal environment [206, 220, 226, 235-237]. This is not a surprising conclusion, given that criminal environments that are populated by prolific offenders remain resilient due to their ability to adapt to the actions of law enforcement and security organisations, as has been noted in the movement of digital vendors to other online marketplaces, and moving into the physical space in the wake of the closure of Hydra in 2022 [240]. This resilience is further exemplified by document forgers adapting to changes in security features and document templates [51], and exploiting weaknesses in digital verification systems, such as the recent use of artificial intelligence (AI) generated images of identity documents [241].

Contrasting to this research, and the clear indication that the cryptomarket criminal environment (like most criminal environments) is resilient and adaptable, the closure of Hydra in 2022 clearly illustrates the risks involved when authorities allow large cryptomarkets to operate unchecked for extended periods of time. The largest cryptomarket in the world, Hydra, was allowed to flourish free from police intervention for 7 years before it was shut down by a

joint American German law enforcement operation [229]. During its time it grew to a size that well exceeded any market that has operated in the United States or Western Europe [229], so its closure understandably created shockwaves that were felt through the cryptomarket criminal environment. The removal of dominant and competitive marketplaces, such as Hydra, can cause extensive competition with the remaining marketplaces, as has been noted in previous studies, and Goonetilleke et al. (2023) hypothesises that this competition serves to destabilise the online drug trade, resulting in increased market-to-market conflicts, DDoS attacks and hacking causing further market casualties without further expenditure from governments [229].

This study by Goonetilleke et al. (2023) highlights how police crackdowns can have a positive impact on the online drug trade, and how a lack of law enforcement engagement can result in unprecedented market growth. However, this does not detract from the previously illustrated resilience of online darknet marketplaces, with it being stated that "…darknet markets have largely recovered after Hydra's closure…" (Chainalysis, 9th Feb 2023 [240]). By their very nature, criminal environments that are populated by prolific offenders are resilient and adaptable, but that isn't to say that police crackdowns should be overlooked. Rather by using these marketplaces as sources of information from a forensic intelligence perspective in combination with targeted police takedowns, the analysis of these markets can be used to simultaneously improve the understanding of these dark web marketplaces, and the larger criminal environments that they contribute to, while ensuring that significant threats can be neutralised through police action. The cryptomarket economy is embedded within and moulded by the customs jurisdictions, economies, and markets within which the users exist, so it stands to reason that investigating the structure, vendors, products, and trafficking patterns of the products within the market, can provide useful information about the overall market for illicit goods.

3.1.5 Cryptomarket research

Since the emergence of Silk Road much research has focussed on exploiting the cryptomarket environment, examining the structure, trafficking and vendor behaviours within marketplaces to gain insight into the criminal environment, mostly focussed on the illicit drug market (for example; [96, 103-107, 110, 117, 203, 217, 220, 221, 223, 235, 242-256]). This research has also expanded into other areas of the illicit marketplace including, but not limited to, firearms [257-260], counterfeit goods and currencies [261, 262], illicit antiquities and wildlife goods [263-266], contracted violence [267], fraud and cybercrime related items [236], and of most relevance to this work, the market for personal information and identity documents, referred to as the ID-related market [201, 202, 268].

So far, there has been no study (published in English) that has conducted a detailed examination of the structure, organisation, trafficking patterns, and vendor behaviours of the cryptomarket facilitated ID-related market, especially not to the depth that has been done for the illicit drug market. Most studies have been conducted on single marketplaces, such as the work conducted by Baravalle et al. (2016) [202] and Degeneve et al. (2022) [201]. These papers are first steps towards understanding the document fraud criminal marketplace. Both these research works provided an overview of the market, but had a stronger focus on the types of documents for sale [201], and the examination of the ID-related market within the context of the illicit drug market [202], rather than conducting a deep analysis of the document market itself. Understanding the illicit market and criminal environment for personal information and identity documents is of importance, particularly given the increasing identity crime rate in Australia and internationally, combined with the fact that identity information and documents are key enablers of organised crime and terrorist activities [29, 32, 51].

Those works that have conducted a deeper analysis of the online fraudulent document market, have extended the scope beyond just examining the cryptomarket-facilitated document trade, to consider vendors that are operating across the open and dark web, including those that operate outside of established cryptomarkets [199, 200]. Holt and Lee's 2020 analysis illustrated the structure of the market, the products for sale, and trends relating to the shipping origin of the documents. They also examined the behaviour of the vendors and their interactions with their customers, including methods of communication and operational structure. Interestingly, they identified that the most sold and listed products were passports (40%), followed by identity cards (25.3%) and driver licences (19.6%), and documents from European (EU) member states (51.2%) and Asia (11.7%) [200]. While this work conducted by Holt and Lee provides great insight into the online market for fraudulent documents, the data examined is skewed toward those vendors operating on the open web, examining eleven vendors of this kind, and eight vendors that were operating on the dark web, only three of which were from cryptomarkets [200]. This high number of vendors and sales from within the open web portion of the online market for fraudulent documents and individual sellers on the dark web could mean that the overall conclusions are not representative of the cryptomarket environment, and therefore the online market as a whole. This is compounded by the fact that the analysis was done on 19 vendors across the open and dark web, which is a small sample set [200].

The online fraudulent document market, without a doubt, exists across a broad range of web-based locations, both on the open and dark web, resulting in quite a scattered criminal environment that is difficult to encompass within one study. Romagna (2015) examined fifty websites and blogs and contacted 65 vendors, all of which produced forged identity documents from across the open and dark web [199]. In their research they organised the vendors that they examined into three groups based on their activities and on what part of the web they operated. The first two groups they identified were those sellers that managed their own online shop

front, either as a website or a blog (present on both the open and dark web) and those sellers that operated primarily through email, spamming forums with advertisements of their products. They identified that a significant portion of the listings and sellers in the online market for fraudulent documents were scams, with 85% of the examined email sellers being con artists [199]. Interestingly, while the legitimacy of the cryptomarket vendors was not quantified in Romagna's work, they did establish that there were typically higher prices for the products offered in the cryptomarkets, likely as a response to the presence of feedback, increasing trust between buyers and sellers, and a perceived higher quality product [199]. Again, this work provides an overview of the online market, considering vendors operating across both the open and the dark web, but it does not provide a detailed description of the organisation and structure of the cryptomarket trade.

Most of the research within the online market for fraudulent documents has provided a great introduction to the overall structure of the market, with quite a few papers examining the whole market, including what is present on the open web, rather than delving into depth regarding the cryptomarket facilitated side of the market. Those works that did examine the cryptomarket trade, did so in less detail, providing a very general understanding of some of the products offered for sale, and some information about vendor behaviours and shipping, without conducting a fully formed analysis like what has been conducted on the illicit drug trade. Aside from this lack of specific detail, most of the papers focus on the presence of counterfeit or 'fake' identity documents, neglecting other parts of the ID-related market that can not only be used as precursors to create fraudulent identity documents, but also facilitate identity crime.

The illicit market for ID-related products, being fraudulent identity documents, their components, and personal information, is important to understand, not only because these items often enable other types of serious and organised crime [32] but also because of the strong

identity crime climate internationally and within Australia [29-31, 47] as explained in Chapter 1 Section 1.3. Contrasting with the results of the work by Holt and Lee [200] and Baravalle et al. [202], more recent research has revealed that Australian identity credentials are some of the most sought-after documents on the dark web [47, 51]. This in combination with the prominent position that Australia holds within the illicit drug cryptomarket environment [104, 110, 117], makes attempting to understand the prevalence of Australian identity documents, and what role Australia plays in this ecosystem of great interest.

Research into the illicit drug criminal environment has pretty consistently identified that cryptomarkets are dominated by English-speaking countries such as the United States, United Kingdom, and Australia [117], with Australia being the second most stated shipping country within the illicit drugs category (following the U.S.) on Silk Road 2.0 and Evolution [104]. On another significant market, Agora, it was found that Australia had the largest number of vendors on a per capita basis [110]. In all cases, it has been found that the illicit drug market in Australia is largely domestic, hypothesised to be as a result of stricter border controls and geographic isolation [104, 110, 117]. All this and more, has provided crucial information to the intelligence community, increasing the understanding of how illicit products move internationally, and within Australia.

Previous research has illustrated the utility of cryptomarkets in providing a broad overview of illicit marketplaces (specifically, the illicit drug market for example; [96, 103-107, 110, 117, 203, 217, 220, 221, 223, 235, 242-256]).), even in cases when the cryptomarkets do not capture the entirety of the online market/demand. Thus far, research into the fraudulent document market has focussed on more specific analyses, targeting vendors individually, or focussing mostly on open web or single shop vendors [199, 200, 269], rather than providing a broader

understanding of the market and the items listed for sale, leaving a significant portion of the criminal environment in the dark.

Given the previous success in illustrating the illicit drug trade, coupled with Australia's prevalence within this criminal environment [104, 110, 117] and the lack of research into the cryptomarket facilitated trade of fraudulent ID's, the cryptomarkets were deemed the most relevant and efficient way of gaining a more comprehensive initial understanding of this portion of the criminal environment. Part of this consideration is the way in which sales volume can be measured and estimated through sales and feedback data (when available). Of course, as outlined above, there are numerous potential data sources that could be used to gain insight into illicit marketplaces, including but not limited to applications like 'Telegram'. However, it was deemed that these more targeted, specific data sources are better suited for a subsequent, more targeted, investigation.

As such, this work will examine two cryptomarkets, to help illuminate the cryptomarket facilitated online market for fraudulent documents and personal information. This will be accomplished through examining the listings, sales, prices, vendor behaviours and trafficking patterns of both the overall market (general products) and ID-Related products with a specific focus on Australian documents, and the Australian market. The supply and demand of the documents (identified through the number of listings and sales) can illustrate the most readily available, and therefore exploitable documents and which are the most popular among buyers. This can indicate what document types may be targeted due to perceived security weaknesses, and which are the most sought after by customers, due to higher perceived value and/or benefits. Overall, this information can provide a much fuller picture of this online criminal environment, and much like with the illicit drug market, can be examined to help disrupt, reduce, and prevent the manufacture and distribution of ID-related products.

3.2 Aims and objectives

This chapter focuses on examining the cryptomarket facilitated portion of the online fraudulent document market, to gain insight into the market, as well as examine trends in supply, demand and trafficking of these products. Two markets, Empire Market and WHM are examined, and the following objectives are addressed:

1. To provide insight into the online identity-related market by examining its size, structure, and trends in products offered, sold, vendors and the trafficking of goods from both an international and Australian perspective.
2. To determine if the online identity-related market is organised, and if it's analysis can be used to better understand the criminal environment for document fraud and identity crime, and assist intelligence-led policing

3.3 Materials and Methods

3.3.1 Dataset

The two markets examined in this study are Empire Market (also referred to as Empire) and White House Market (WHM).

3.3.1.1 Data collection and ethical considerations

The Hyper-text Markup Language (HTML) of all active listings and pages from each cryptomarket was crawled[17] using dedicated crawlers developed for each cryptomarket and was conducted by an external collaborator at the University of Lausanne (UNIL), Switzerland. This data was then sent in the form of .csv files for analysis.

The crawling and collection of the data was covered under ethics application number C_FDCA_022022_00009 granted by the University of Lausanne, Switzerland. The information that has been analysed within this research was collected from the publicly available information within these cryptomarkets. By its nature, the cryptomarket environment is anonymous, and no personal information of the vendors or users was crawled as part of the collection procedure. To ensure that no vendor can be identified, all usernames were anonymised, and no personal information or profile data was included in the analysis. The data that has been collected has been done so entirely for research purposes, and in no way poses any risk to any users of these marketplaces.

3.3.1.2 Empire Market

Empire Market was launched around February of 2018 and, at its peak, had approximately 1.3 million users and was considered one of the largest dark web markets at the time prior to its closure in August of 2020 [270, 271]. It later surfaced that the market hadn't simply closed,

[17] The automated process of using a computer program to search, collect, and index web page content and information [205].

but rather the administrators had exit scammed, stealing approximately $30 million (USD) from its users. During its operation, it was estimated to be generating $6.5 million (USD) in sales per week [270, 271]. Empire Market was crawled eight times over the period between June and August of 2020, the latest being the 12th of August, shortly before the market's exit scam. The webpages of the advertisements were extracted and then cleaned (including the removal of duplicates and incomplete listings), resulting in 79,397 unique listings and 2,806 distinct vendors.

3.3.1.3 White House Market

WHM was launched in August of 2019. Until its closure in October 2021, it was known for its excellent security, customer service, and, most interestingly, its ethics as the administrators did not allow the trade of child pornography, murder for hire, weapons, explosives or poisons [272]. While it did not reach the sales volume or size of its predecessors like AlphaBay, WHM had established itself as one of the more popular dark web marketplaces [243, 272]. At the time of its closure, it had approximately 900,000 registered users and was estimated to have facilitated between $35-120 million (USD) in sales before its voluntary closure by administrators, stating that they had "reached [their] goal" and that the shutdown was "according to plan" [273]. During its operation, WHM was crawled thirty times, across eight months of 2020 and three months of 2021. The webpages of the advertisements were extracted and then cleaned (including the removal of duplicates and incomplete listings), resulting in 83,517 unique listings, and 2,519 distinct vendors.

The dates that both Empire and WHM were active, along with the dates that the markets were crawled is summarised in Figure 3-2. Even though both WHM and Empire Market are no longer active and therefore may be considered as 'irrelevant', their analysis can still provide valuable insight into the criminal environment [104], especially as both markets grew to a

significant size, both in relation to number of users and the number of sales that they facilitated [270-272]. It is also common within forensic intelligence to analyse cryptomarkets after they have closed [96, 104, 117, 203, 247].

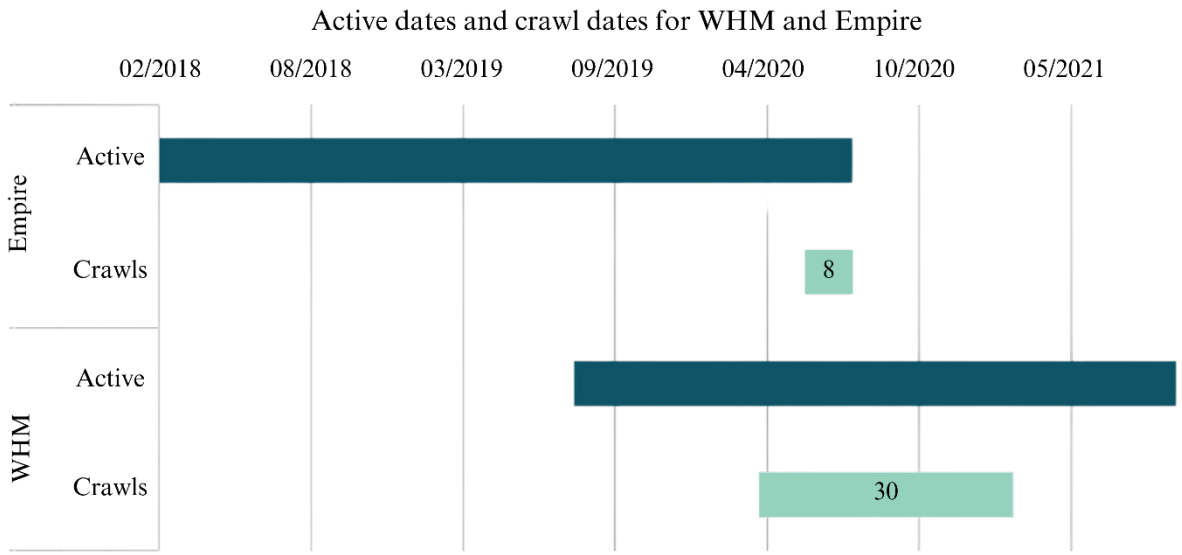


Figure 3-2: Summarised active dates and crawling dates for both Empire Market and WHM

3.3.2 Data extraction and wrangling

For each listing, the product ID number, title, description, price (in USD/EUR), vendor name, vendor ID number, profile description, feedback, product views, shipping information, product category, and in the case of Empire Market, number of sales, was extracted. The prices of items in USD and EUR were converted to AUD using the average conversion rate across the crawling periods using data extracted from exchangerates.org[18].

While the number of sales was available for Empire Market, no such data was available for WHM, so any sales calculations on WHM would rely solely on the feedback data. To investigate whether the feedback on WHM could be used as a proxy for the number of ID-related sales the total amount of feedback for the ID-related market was examined, along with

[18] https://www.exchangerates.org.uk/USD-AUD-spot-exchange-rates-history-2020.html

the ratio of feedback to sales on Empire Market. On WHM there was only 1,062 instances of feedback for ID-related products, out of the 364,560 reviews left across the overall market (0.29%). To provide some more context, the ratio of sales to feedback received for ID-related products on Empire Market was investigated, and it was found that only 8,567 (17.6%) sales had feedback associated, perhaps suggesting that feedback, particularly within these marketplaces, is not a reliable proxy for number of sales within the ID-related market.

Previous research, focussing largely on the drug market, has illustrated that only 60-90% of the transactions on dark web markets typically receive feedback [203, 218, 249, 250, 274]. In marketplaces where it is not compulsory for buyers to leave feedback, it is a less reliable proxy for sales [218] as the likelihood of a buyer leaving feedback is largely dictated by the culture and customs of the market and the buyers. The drug market for example has a strong feedback culture, undoubtedly because of the types of products being purchased and the increased safety and fraud risk associated. Many markets have used integrated community forums to facilitate discussions among customers regarding products they had purchased and their feedback [275]. This combined with the increased tendency for repeat customers has created a strong feedback culture within the drug market on cryptomarkets.

In contrast to this, when considering the validity of feedback as a proxy for sales in the ID-related market, while no solid conclusion can be made at this stage, it is reasonable to consider some hypotheses as to why there may be less feedback left on ID-related products. Aside from the safety concerns and an associated moral imperative related to leaving feedback for drug related products, it is hypothesised that there is a smaller demand for fraudulent identity documents on a per client basis, with clients usually purchasing one fake identity document at a time [13, 51]. This contrasts to the drug related market, where there are more likely to be regular purchases either for medical reasons (i.e. prescription drugs), to support an addiction

or as a means of recreation. Additionally, there may be an increased delay between receiving the identity document and knowing whether it works, as this can only be tested through successfully using the identity document to pass an identity check. While impossible at this stage to determine the precise reason behind the decreased amount of feedback on the ID-related market, the hypotheses above are just potential explanations. Given that on Empire only 17.6% of sales had feedback associated in combination with the low number of reviews for ID-related products on WHM, it was determined that the feedback on WHM would not be used as a proxy for sales, and that the sales information from Empire would be the focus instead. While this is a limitation, previous studies have suggested that single-market studies are still valid and can provide generalised results about the overall marketplace [104, 218, 242, 250], which is especially relevant as Empire Market and WHM were contemporaries.

3.3.3 Classification of listings

The product category as dictated by the vendor was extracted, however, in cryptomarket research it is often found that vendor-selected categories are incorrect, or not relevant for research [104]. To ensure comparisons were consistent across the markets, and irrelevant products were removed from the analysis, listings were re-classified using a semi-automatic keyword macro as done in previous research [96, 104, 117]. This macro was optimised in this study for the ID-related market, identifying keywords of importance by studying the fraudulent document literature (for example [47, 51, 200]) along with the product titles of the listings. This was an iterative process of running the macro and adjusting the search terms, thereby reducing the amount of manual classification required. For the items outside of the ID-related category, this was expedited through using the vendor selected category to help with bulk classifications that were then checked after the fact. There may be some level of error with this method, but this was deemed acceptable as the focus of this research was the ID-related market. After all listings were classified, the items that fell within the ID-related category, including

both identity documents and identity fraud-related products were extracted, with 2,545 unique listings and 234 vendors on Empire, and 1,620 unique listings and 141 vendors on WHM. The different categories used for the ID-related products can be found below in Table 3.2.

Typically, fraudulent documents are categorised by vendors as part of either the 'services' or 'counterfeits' category. While these products could be considered part of the fraud category, for clarity, within this research they have been allocated their own category. The fraud category is expansive, including a broad range of products, which should be broken down into more specific categories to allow a better understanding of the overall market. All products that were related to identity documents or proof of identity documents, including things that could be considered 'precursors' such as fullz (defined in Table 3.2), have been added to the ID-related category in this research.

Table 3.2: Summary of the different categories used to classify the ID-related product listings, these definitions were developed specifically for this research

Product category	**Product**	**Definition**
ID	Licence	A document that can be used as a proof of identity, and proof of entitlement to drive. It contains an image of the individual along with a range of personal information
	Passport	A document that can be used as proof of identity and to travel across borders. It contains an image of the individual and personal information
	Identity card	A document that can be used to prove the identity of an individual, it contains an image of the individual and personal information (e.g. proof of age cards in Australia)
	ID pack	An ID pack is used to describe a collection of two or more documents of different types often curated to serve a specific

		purpose, such as proof of identity to secure a bank loan or opening a bank account.
	ID bulk	A bulk listing for multiples of the same document types (e.g. 10x passports, 1000x licence scans)
	ID various	This product type was used to describe listings that had multiple different document types within the listing but were not being sold as a pack. Rather the vendor was offering all those products within one listing, and the buyer would need to specify what document they wished to purchase.
	Selfie ID	This product type is an image of an individual holding up an identity document such as a driver licence or passport
	Other	This was used to group all other ID that did not fall within these previously mentioned categories, but were not numerous enough to create their own category (e.g. ID components such as barcodes and other security features and tools to manufacture the documents, such as card printers, barcode generating software etc.)
Identity fraud	Fullz	The 'full' information profile of an individual. This is sold as a digital packet that contains personal and financial information and is often used to facilitate identity fraud, bank drops, credit card fraud etc. It will often include things such as a name, date of birth, address, email address, credit card information, bank information, drivers licence number, and sometimes even a physical description
	Identity fraud pack	This has been used to group listings for fullz that are sold in combination with an identity document, often a scan or image, as opposed to just a document number.
	Other	This product category includes things that assist in the creation of fullz, for example, 'look up' services for driver

		licence information, dates of birth, and social security numbers
Various legitimation documents	Statements	This contains all listings that include the word 'statement' such as bank statements and tax statements.
	Utility bill	Any form of bill, including gas, water, electricity, phone etc.
	Other	This category contains all other documents that did not fit within the previous categories. This includes things such as birth certificates, social security cards, Medicare cards, insurance cards, and residence permits

3.3.4 Data analysis

3.3.4.1 Overview and structure of the international market

The overall illicit marketplace of WHM and Empire Market were examined to place the ID-related market within its context. To illustrate the supply and demand of the overall illicit and ID-related markets the number of listings (based on unique product ID numbers) and the number of sales (only on Empire) were used, along with the number of vendors, identified through the vendor usernames. The number of sales and listings was then identified for each product type within the markets. When examining the number of sales, it was identified that some listings were incomplete, in that they were missing the number of sales for that item, likely due to errors in the crawling, or incomplete crawling. In these cases (n=3,215), the listing was removed from the sales calculations. Typically, when there is no stock left of an item, cryptomarket vendors will greatly increase the items price to dissuade buyers [104, 218, 276], indicating in the product title or description that they are sold out. When this was identified those listings were not included in the price, nor the calculations for total sales revenue (n=37).

Specifically for the ID market, when an item's price was significantly higher than the average price for that item, they were removed from the total sales calculations (n=6). This was done

manually on a case-by-case basis, using knowledge of the market and prices published in previous research [47] to inform the decision. One such item that was removed from the sales calculation was a digital scan of a driver licence that was listed for close to $7000, when the average price was $31.40. The total sales value per item, along with the estimated value of the overall and ID-related markets on Empire were estimated by first converting the price (in USD or EUR) to AUD as described above (Section 3.2.2), and then multiplying that by the number of sales as was done in previous research [104, 247]. The number of sales was the number of sales since the vendor joined the market, or in the case of individual items, since that item was listed, and this calculation was done to give an indication as to the revenue for individuals, vendors and the market as a whole across the duration of its operation. The total sales value for every item in the ID-related category was then summed together to estimate the total value of the ID-related market on Empire across the time it was active. Of course, there may be some inaccuracies in this analysis, particularly if there have been price fluctuations across the duration of the market's operation, but the revenue has been provided as an estimate to give an indication as to the potential revenue of individual vendors, products as well as the overall market

3.3.4.2 Identification of digital products, document country, and fraud type

Previous research has illustrated that the ID-related category had a significant number of listings for digital items [104], so to determine the number of digital listings present on WHM and Empire, the keyword macro used to classify the product categories was modified to classify the listings as either digital or physical, based on the presence of keywords in the listing title. This macro targeted words such as 'scan', 'template', 'image', 'fullz', and 'PSD' to identify those documents that were in a digital format. The same keyword macro was also used to identify the document country for each listing, being the country the document was claiming to be from or attempting to replicate (e.g. Australian vs United States passports). In this

instance, the macro targeted words associated with countries, states, or regions around the world, including common abbreviations. As an example, if a listing contained the words 'New York' or 'NY' then it would be classified as a listing for a United States document. In cases where vendors indicated multiple document countries or regions within a single listing (e.g. Europe, Oceania, Asia etc.) those documents were given a document country of 'Various'. When no document country was included in the listing title they were classified as 'Not Specified'. As the 'Not Specified' document countries provided no real information about the document, they were not included in the examination of the document country, resulting in the exclusion of 573 listings from Empire (22%) and 378 listings from WHM (23%).

The key word macro was again modified and used to identify the types of products being offered by vendors, and what type of document fraud was being committed, i.e. counterfeit vs. forgery. The key word macro, however, was not effective for the classification of the fraud type, as there was a high degree of variability in the way this information was conveyed by the vendor, with some not explicitly stating it in the product title, and instead including it in the product description, or alluding to it. For this reason, manual classifications were conducted by extracting information from the product listing title and description. Only the physical documents were targeted, as in most cases this information was not provided, or was not reliable for the digital document listings. The number of listings, sales, and total sales value (AUD) per fraud type was calculated as outlined in Section 3.2.2.

3.3.4.3 Trafficking of products

To get an understanding of the movement of illicit goods internationally, and therefore the trafficking of goods within the market, the shipping information provided within the ID-related market was examined.

Across both WHM and Empire vendors provided their shipping locations, being the places that they ship items from and where they ship to. Previous research has indicated that it is reasonable to assume that the country the item is being shipped from (i.e. the origin) is the country of operation of the vendor, so that approach has been followed here [103, 104, 110]. While it is not possible to verify that this information is completely accurate, as feedback and reputation are some of the most important currencies on the cryptomarkets the threat of receiving bad feedback from a customer is likely enough motivation to be honest regarding the origin country of the product [110, 117]. On Empire, some vendors indicated a list of countries that they ship to, in which cases the lists were separated to ensure that the countries were correctly represented.

All digital products were removed from the geographical analysis (Empire n=2,022 listings and n=44,979 sales, WHM n=1264 listings), as the shipping information provided for digital products is less reliable as it cannot be verified by the buyers [117]. Any listings that had both the origin and destination country listed as 'Worldwide' were also removed from the analysis (Empire n=240 listings and n=1,088 sales, WHM n=33 listings). The trafficking analysis was therefore focussed on 189 listings and 552 sales from Empire and 323 listings from WHM. The origin countries were first examined, contrasting this against the products offered for sale, after which Alluvial Sankey diagrams were used to illustrate the flow of products from the origin to destination countries.

3.3.4.4 Vendor behaviours

The number of sales and listings per vendor, in combination with their total sales revenue (AUD), was used to identify those vendors that were making the most significant contribution to the ID-related market. It is common practice within cryptomarkets for vendors to migrate and operate across different marketplaces, either as a reaction to the closure of a market, as a strategy to reduce risk [236], and/or to expand their reach thereby increasing their likelihood

of higher profits [226, 277]. As a vendor's username is intrinsically tied to their reputation [220, 226, 278] previous research has illustrated that usernames can be used as a proxy to help in the identification of vendors that are operating across different marketplaces, albeit with a degree of uncertainty [220, 226, 236]. However, this uncertainty can be mitigated by pairing the comparison of the vendor's username with the comparison to their PGP key [203, 279]. After the PGP keys were cleaned to remove formatting inconsistencies between the markets, a vendor comparison using their username and PGP key was done to identify which vendors were present across both markets.

All data extraction, wrangling, and classifications were conducted using Microsoft Excel for Microsoft 365 MSO Version 2401. All data analysis was conducted using a combination of Microsoft Excel for Microsoft 365 MSO Version 2401, Tableau 2023.2, and Flourish Studio[19].

[19] https://flourish.studio/

3.4 Results and Discussion

3.4.1 Overview of the illicit marketplaces

3.4.1.1 Market categories

While cryptomarkets often vary in appearance, they are similar in the way that their products are organised, utilising product categories to make searching and purchasing easier from a consumer perspective [255]. After the data wrangling and categorisation process, there were 76,182 listings and 2,806 vendors on Empire Market and 83,517 listings and 2,519 vendors on WHM. Figure 3-3 compares the number of listings and the number of vendors per market category across both Empire and WHM, with the number and percentage of the market included on the bars. These are referring specifically to the percentage of the individual market, not both markets combined. All market categories have been defined in Appendix Table A. 9.

Unsurprisingly, the market structure is very similar across both WHM and Empire, with most of the listings and vendors being within the illicit drugs category (63.7% and 48.6% for WHM and Empire respectively). Previous research has found that most cryptomarkets will operate with between 46-57% of their listings being devoted to illicit drugs [104, 249]. While Empire fits within this expected range at 48.6%, WHM does have a higher percentage of listings at 63.7%. During its operation, WHM garnered a reputation for being a market that had a focus on the sale of illicit substances [273], which was undoubtedly furthered by the branding of the market as shown in Figure 3-4.

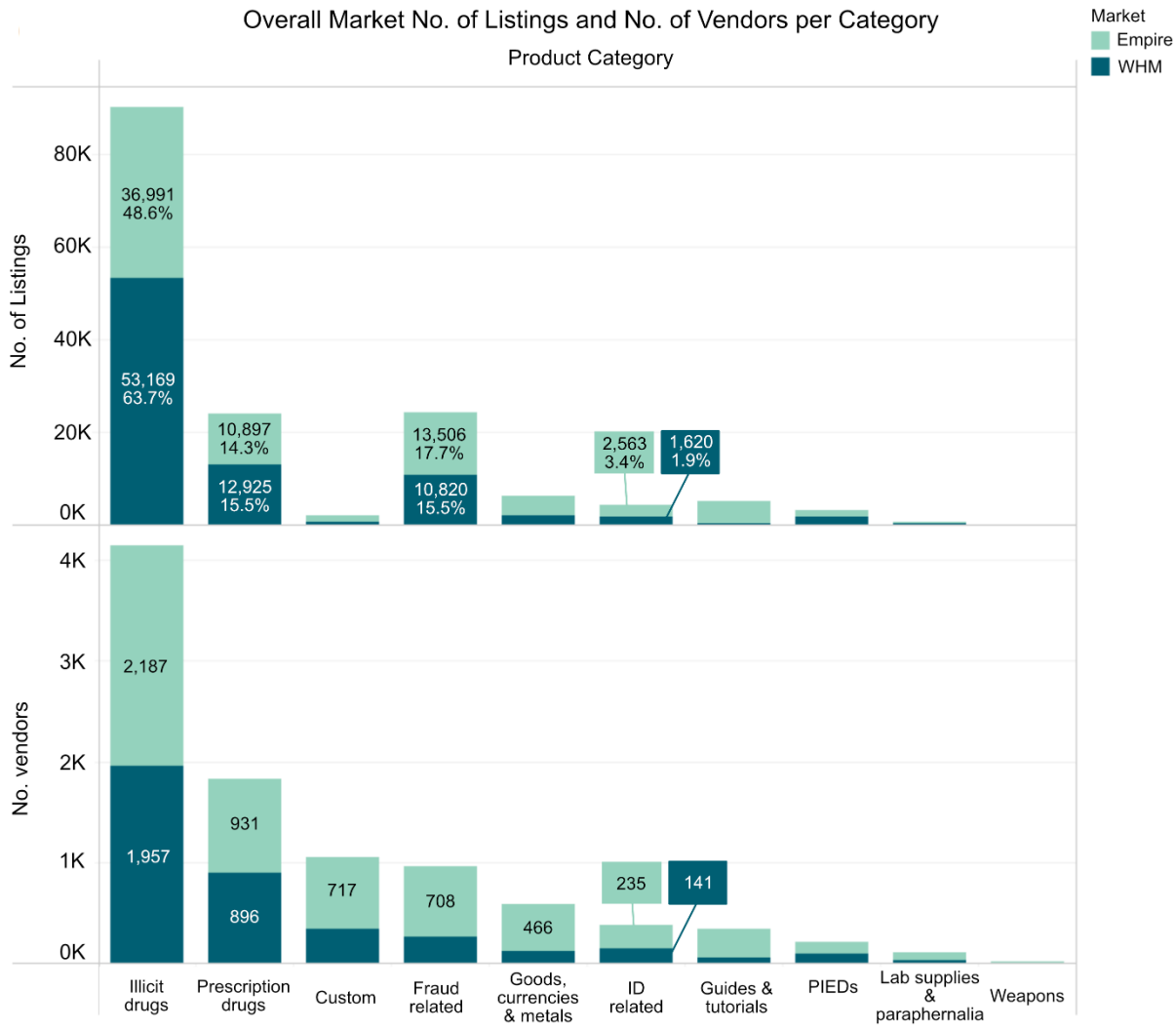


Figure 3-3: Number of vendors and number of listings per market category compared across both WHM and Empire. The light aqua correlates to Empire while the dark teal correlates to WHM. The percentages for the number of listings here are referring to the percentages of the individual markets, not both markets combined. Percentages were not used for the number of vendors as most vendors appear in multiple categories. Note: PIEDs = performance and image enhancing drugs.

Figure 3-4: The branding for WHM, featuring Walter White, the character from Gilligan and Johnson's Breaking Bad (https://thecyberpost.com/news/cybercrime/darkweb-news/white-house-market-ends-support-for-bitcoin-payments/)

When looking at the listings on Empire there appears to be a stronger emphasis on the fraud related category, than there is on WHM, with it being Empire's second most listed category. As most of the products in this category are digital products (for example software and dumps of information) it is unsurprising that they take up a large portion of the listings on the market due to their ability to be reused, modified, and resold, unlike the typically physical products within the drug related category.

Across Empire and WHM, during the crawling period, there were, respectively, 2,808 and 2,519 active vendors. Across both marketplaces, approximately 78% of these vendors had product listings that fell within the illicit drug category, making it by far the most populated category on both markets. The trends regarding the number of vendors largely followed the same trends noted for the number of listings, with illicit and prescription drugs and fraud-related taking up most of the market. However, there was a startling difference when considering the number of vendors in the 'custom' category. It should be noted that the 'Custom' category contains products from all the other categories but seems to be very common for drug and fraud-related products. This breadth of the custom category may be an explanation as to why so many vendors fall within this category, even though the number of listings is comparatively small.

The number of listings provides a good indication of the supply across the market, i.e. what product types are being listed by vendors, however, this is not an accurate indication of what products are being purchased by buyers. Previous research has used feedback as a proxy for the number of sales when sales data has not been available, most often due to the structure of the market [256]. However, as the feedback on WHM was not representative of the ID-related market (as outlined in Section 3.2.2) this was not used, and instead the sales information from Empire Market was used as a more accurate indicator for the demand across the market.

On Empire, there were 2,065,815 sales and an estimated total sales revenue of $362,178,498 (AUD[20]) across the time the market was operational, until the final crawl. Here, the illicit drug category is once again dominating the market, with over 50% of the sales and 72% of the revenue coming from illicit drug listings. The trend for the top three product categories regarding the number of sales is consistent with the number of listings, with fraud-related being the second most sold followed by prescription drugs. However, regarding the other categories, there have been some notable shifts with guides and tutorials and ID-related moving up to fourth and fifth place respectively in the number of sales, as illustrated in Table 3.3

[20] All sales revenues and prices in this analysis are in AUD unless mentioned otherwise

Table 3.3: Number of sales and sales revenue for each category across Empire Market

Category	No. sales	Sales revenue
Illicit drugs	1,105,378	$265,303,894
Fraud related	330,992	$14,957,650
Prescription drugs	302,023	$62,256,966
Guides & tutorials	202,732	$4,558,693
ID-related	48,655	$1,823,485
Goods, currencies & metals	41,285	$8,010,715
PIEDs[21]	19,189	$1,240,090
Custom/other	12,671	$3,930,677
Lab supplies & paraphernalia	2,496	$90,356
Weapons	394	$5,974
Total	2,065,815	$362,178,498

There are some interesting differences when looking at the number of sales against the total sales revenue. The categories that are dominated by physical products, such as the illicit and prescription drug categories, generally have much higher total sales revenues, regardless of their number of sales. The other categories, particularly those with a larger portion of digital products such as fraud related, guides and tutorials, and ID-related, all have a much lower total sales revenue. Digital products have a much lower cost per unit compared to physical products [47], thus explaining the differences between the number of sales and total revenue for these primarily digital categories.

Based on the structure and organisation of the overall markets for both Empire and WHM, it is apparent that these markets are very similar to what has been previously published. The fact that they are exhibiting characteristics that are typical of cryptomarkets is a good indicator that

[21] Performance and image enhancing drugs

the identity-related market within these two cryptomarkets may be a good example of the typical cryptomarket facilitated ID-related market.

3.4.1.2 Market structure

The identification of prolific offenders operating on the cryptomarkets can assist with not only illustrating the structure within these online markets but also could provide an alternative way of disrupting this persistent criminal ecosystem. Given the reported resilience of these markets to disruptions such as police takedowns [203, 206, 220, 221, 236], it has been suggested that rather than targeting markets, which are promptly replaced, security and policing organisation should consider targeting the more prolific offenders, being those individuals that are having a large impact on the supply and sales within the marketplace [247]. However, as illustrated through the closure of Hydra market in 2022, police crackdowns are necessary to keep these growing marketplaces in check [229], even if new marketplaces continuously emerge to replace those that are closed. It is important to consider the benefits and potential of both approaches, targeting and removing both key markets, as well as those most prolific and influential vendors. In this work, prolific, in the context of vendor behaviour, is defined as a vendor that is listing, selling, or earning well above the average across the market. The number of listings per vendor for both the overall and ID-related markets were plotted as a histogram (Figure 3-5) to identity firstly, if the cryptomarket environment for ID-related products is punctuated by prolific offenders, and secondly, if this structure is unique to the ID-related market or if it is present in the structure of the overall market.

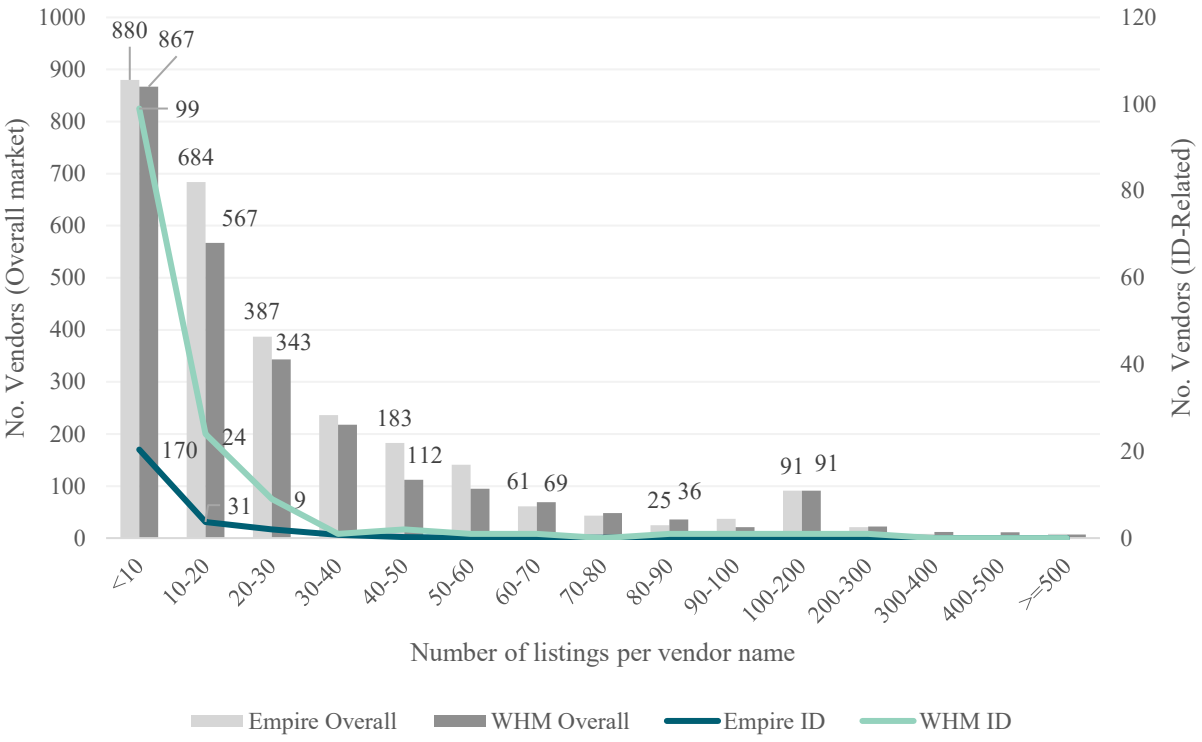


Figure 3-5: Histogram illustrating the number of listings per vendor across Empire and WHM's overall and ID-related market. The columns correlate to the overall markets, while the lines illustrate the ID-related market (e.g. there were 880 vendors in the overall market on Empire that contributed less than 10 listings). Note the axis on the right is correlating to the number of vendors in the ID-related market, the axis on the left is correlating to the overall market.

Figure 3-5 illustrates the number of listings controlled per vendor across the overall market (illustrated by the bars) and the ID-related market (illustrated by the lines). This provides a visual representation of the concentration of vendors within the marketplace, highlighting the number of vendors that can be considered 'prolific'. It is obvious that across both Empire and WHM the structure of the overall market and the ID-related market is similar, with many vendors controlling less than ten listings (overall market: Empire 31% and WHM 34%, ID-related market: Empire 73% and WHM 70%). This is consistent with previous research that found that in an examination of the Canadian drug market across eight different cryptomarkets, 47% of the vendors controlled less than 10 listings [203]. It has been suggested that most vendors may favour operating a small number of listings due to the difficulty of managing

several listings at the same time across a broad range of products, especially when considering that a single listing may be purchased multiple times [203].

Previous research that has focussed on the profiling of fraudulent identity documents has illustrated that the fraudulent document market is characterised by a small number of prolific offenders contributing a large number of documents to the marketplace [1, 14-17, 51, 280]. This seems to be consistent with the online market, with only four vendors (two per market) contributing over 100 listings, which could be considered significantly above the average for both the ID (average of 11 listings) and overall markets (average of ~30 listings).

While the number of listings a vendor controls may be indicative of how large a role they play in the supply of the market [203], this cannot be the only characteristic used to determine which vendors can be considered prolific. When examining the number of sales per vendor on Empire, there is a noted concentration of activity amongst a small number of vendors (Figure 3.6). In the overall market, 16% (460) of the vendors are responsible for over 80% of the sales on Empire, and in the ID-related market, 5.5% (13) of the vendors are contributing 63% of the ID-related sales on Empire. Clearly, this level of concentration and the presence of prolific offenders is not unique to the fraudulent document market (both physical and online) and is instead likely to be present across the entirety of the cryptomarket ecosystem, which is in line with criminological theories of recidivism and prolific offending [60].

To get an indication of the distribution of the sales across the vendors within the ID-related portion of Empire Market, the Herfindahl-Hirschman Index (HHI) was calculated. The HHI is commonly used in finance and economics to illustrate the concentration of a marketplace, and the degree of competition between contributors [281]. Originally developed by Hirschman [1945] and Herfindahl [1950], the HHI is calculated using the formula below and is represented

as a value between 0, indicating a huge number of very small contributors and 10,000, indicating a small number of contributors operating a monopoly [282]:

$$HHI = S_1^2 + S_2^2 + S_3^2 + \dots S_n^2$$

In this calculation, S corresponds to the market share of each contributor (i.e. vendor in this work) and is calculated using the formula below.

$$S = \frac{vendor\ sales}{total\ sales\ in\ ID\ related\ market}$$

Based on this calculation, the HHI for the ID-related portion of Empire Market was found to be 382, correlating to a competitive market, with many vendors contributing to the marketplace. This of course doesn't negate the fact that there are prolific offenders operating within this marketplace, as 50% of the sales for the entire ID-related market on Empire is coming from only 10 vendors (when there are 234 ID-related vendors on Empire Market). Low HHI's are typically indicative of a roughly equal distribution of sales across the contributors to the market [282], and this makes sense in this context given that 199 of the 235 vendors in the ID-related market on Empire (85%) have a market share (S) of less than one, as they are not contributing very many, or in some cases, any, sales to the ID-related market.

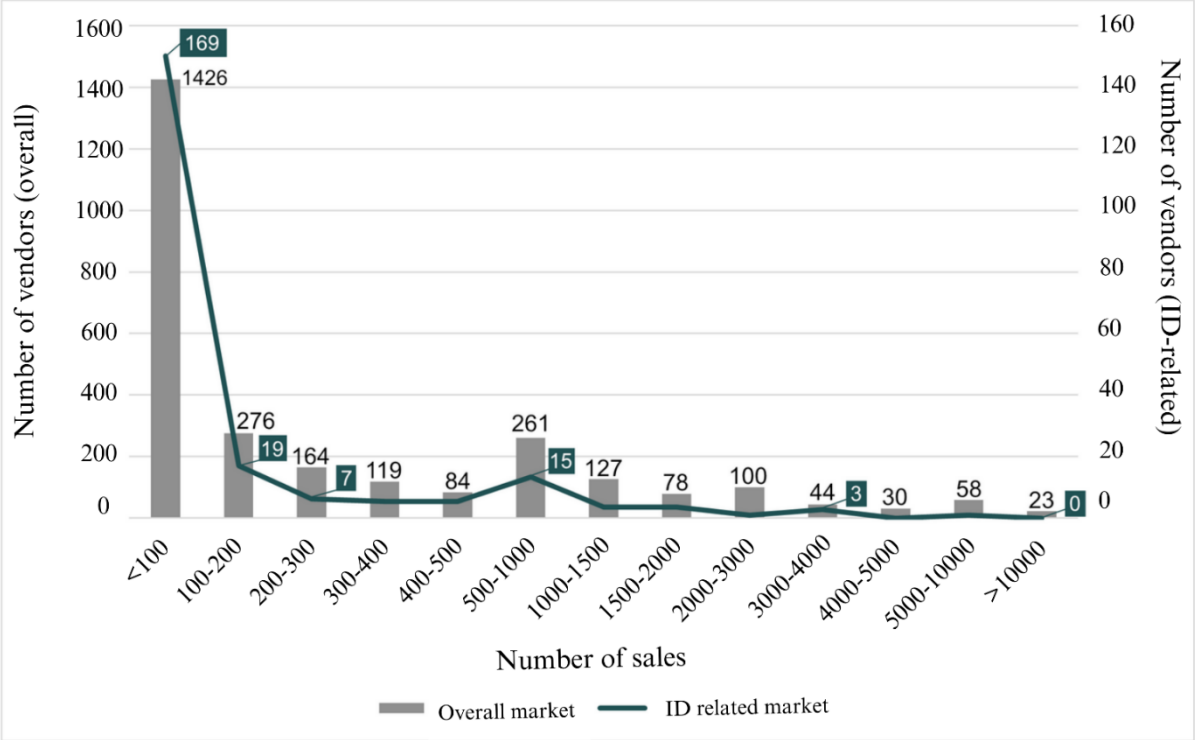


Figure 3-6: Number of sales per vendor across the overall and ID-related market on Empire. The columns illustrate the number of vendors that have that number of sales (e.g. there are 1,426 vendors in the overall market with less than 100 sales).

To properly identify those vendors that can be considered as making significant contributions to this online marketplace, their listings, sales, and total revenue need to be considered in combination. Using one characteristic, such as the number of sales in isolation is neglecting to consider those vendors that may have access to (and therefore be supplying) a large amount of product to the market (identified through the number of listings) and those that are earning a large amount of money from their illicit activities (identified through their total sales revenue). Those individuals that are earning large sums of money are the vendors that are more likely to expand their business, whether that be onto other cryptomarkets, increasing their product profile, or moving into physical markets in combination with the online markets.

The importance of considering sales, listings, and the total revenue when identifying prolific behaviour is illustrated in Figure 3-7. This shows the total sales revenue (y-axis), highlighting the 15 ID-related vendors with the highest sales revenue, along with their number of sales (x-axis) and number of listings (size). The lack of correlation between the number of listings and sales is perfectly illustrated by the vendor with the highest number of sales, who has 5,256 sales coming from six listings, all within the identity fraud-related category. Clearly, to properly capture the activities of the most prolific vendors within the market environment, sales, listings, and sales revenue should all be considered to ensure that information is not being overlooked by focusing too much on only one trace of activity. Of course, much of this is reliant on whether sales data is captured in the crawl and is structured in an accessible way by the market administrators. It should be noted that this analysis could not consider the possibility that a single document supplier may be operating multiple vendor usernames, therefore potentially disguising their prolific activities.

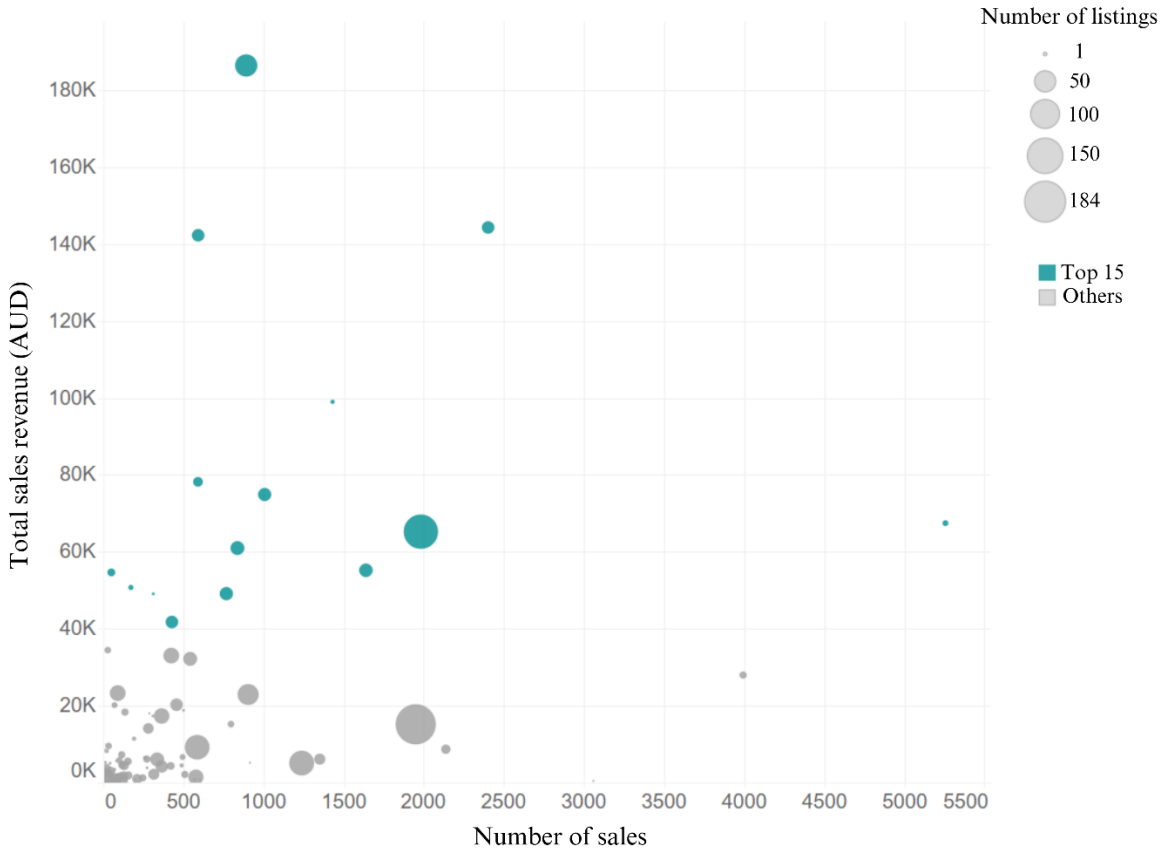


Figure 3-7: Total sales revenue, number of sales (x-axis) and number of listings (size) per vendor with the 15 vendors with the highest total sales value (ID-related market) highlighted in aqua.

3.4.2 The cryptomarket facilitated ID-related market

3.4.2.1 Overview

The ID-related category contains a broad range of product types that, for the sake of simplicity, have been grouped into three subcategories as defined in Table 3.4. For more detailed definitions of all the product types found within each subcategory, refer to Table 3.2 in the Materials and Methods Section 3.2.3.

Table 3.4: Definitions and examples of the three ID-related product subcategories

Product subcategory	Definition	Examples
ID	Photo identification products, those that can be used in isolation to prove an identity	Passport, driver licence, identity card
Identity fraud	Includes all products that could be used to facilitate identity crime or theft	Fullz (a full, digital information pack about an individual), and identity fraud packs, being a pack containing fullz and a document from either of the other categories (ID or various legitimation documents)
Various legitimation documents	Documents that do not contain a photo and cannot be used to prove an identity. They can only support a photo ID, or be used as a proof of address	Utility bills, bank statements, birth certificates

Across the ID-related category, there are 2,545 listings and 234 vendors on Empire and 1,620 listings and 141 vendors on WHM. Most cryptomarkets, including those beyond the scope of this research, typically offer both digital and physical products, being those that are transferred

to the buyer through the internet, and those that require shipping from the vendor to the buyer's address or P.O box, respectively. As illustrated in Figure 3-8, approximately 80% of the ID-related listings across both markets (80% on Empire and 78% on WHM) are for digital products, largely being scans, images, or Photoshop templates (.PSD) of identity documents, along with fullz and identity fraud packs. When looking at specific product types, driver licences are the most listed products for sale, consistent with previous research [47, 51], followed by fullz, then identity fraud packs on Empire, and identity cards on WHM. Driver licences are often targeted products within cryptomarkets as they are widely used throughout communities as proof of identity, and they contain valuable information such as date of birth, name, and address [47]. In addition, in some country's driver licences are attractive as they do not have an expiry date [51, 283].

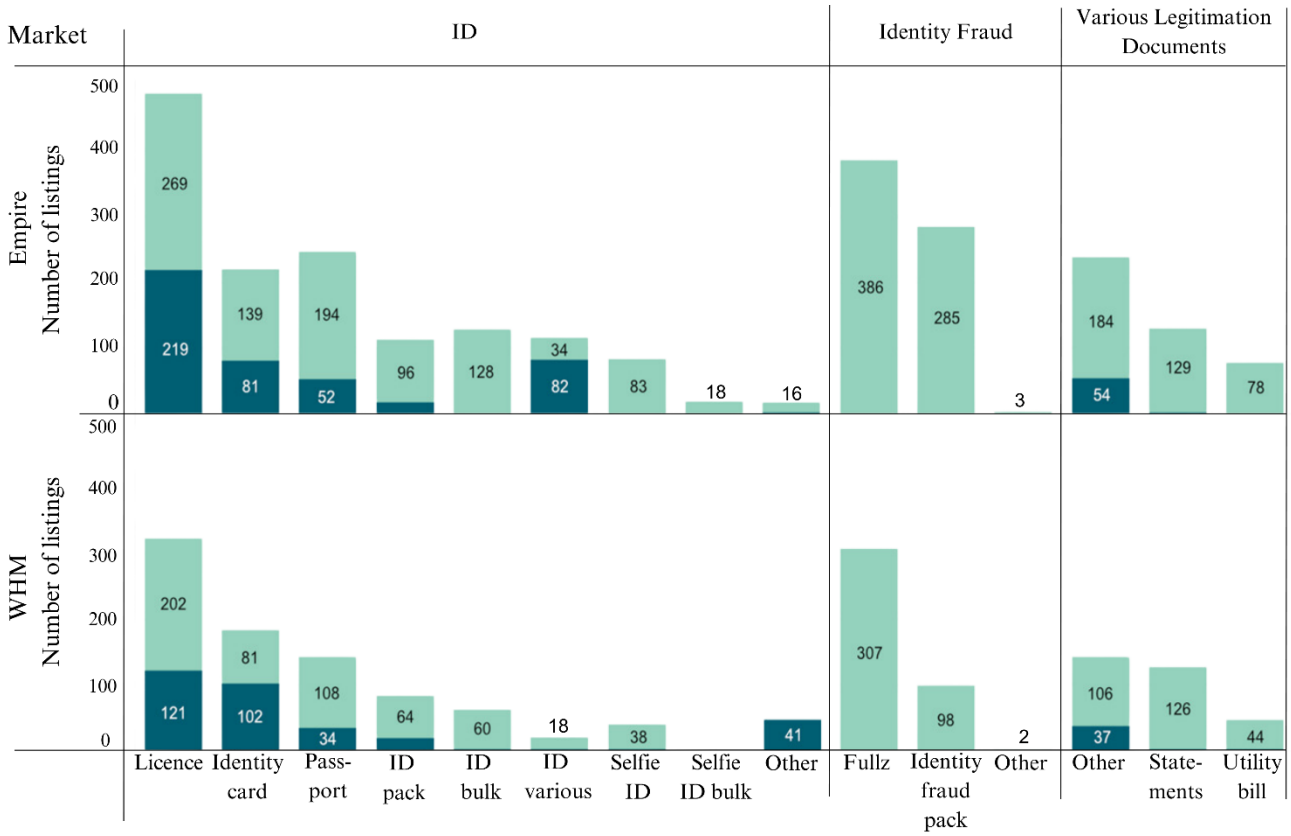


Figure 3-8: The number of listings per product type across the ID-related category for both Empire and WHM, with the colours indicating whether the documents are physical (dark teal) or digital (light aqua).

There were 48,655 ID-related sales on Empire, 95% of which were for digital products, suggesting that there is both supply (indicated by the number of listings in Figure 3-8) and demand for digital products within these marketplaces (as illustrated in Table 3.5).

Table 3.5: The total number of sales and listings per ID-related category and the total sales in AUD (Empire Market)

	Category	No. of listings	No. of sales	Total sales (AUD)
ID	Licence	493	5,653	$402,059
	Passport	245	1,072	$67,204
	Identity card	212	1,164	$189,902
	ID bulk	128	3,980	$70,164
	ID various	118	1,497	$104,836
	ID pack	111	1,024	$65,014
	Selfie ID	83	532	$38,787
	Other	20	125	$14,276
	Selfie ID bulk	18	1	$489
	Total	**1,428**	**15,048**	**$952,731**
Identity fraud	Fullz	384	20,649	$435,345
	Identity fraud pack	286	8,186	$261,094
	Other	3	336	$18,712
	Total	**673**	**29,171**	**$715,152**
Various legitimation documents	Other	237	2,725	$129,480
	Statements	130	1,185	$16,388
	Utility bill	77	526	$9,735
	Total	**444**	**4,436**	**$155,603**
Grand Total		**2,545**	**48,655**	**$1,823,485**

Interestingly, the category with the highest number of sales, the identity fraud-related category, is made up entirely of listings for digital products. This is not surprising given the ease with which digital documents and information can be sent to the buyer, edited, modified, and re-

used, especially if they are taking the form of Photoshop templates, scans, and digital information (in the case of the identity fraud related items). The generally low cost per unit [47] coupled with the increasing reliance on digital proof of identity documents, may also be contributing to the popularity of these items with buyers. Of course, it is entirely possible that these digital documents are being used as 'precursors' and are being purchased for use in the manufacture of physical documents. While not among the most popular products on the cryptomarket, within the 'Other' section of the ID category are what can be considered 'precursors' for document manufacture, including things such as substrates, security features, and security overlays. This, combined with increases in the trafficking of these precursors [51], indicates that the manufacture of physical documents may be a potential use for these digital documents and personal information.

Also contributing to the high number of sales within the identity fraud category, particularly for fullz, is the ever-increasing rate of identity crime that has been noted internationally, and domestically in Australia, as explained in Chapter 1 Section 1.2. It was found in the AIC's 2023 identity crime and misuse report that the most targeted and misused information were personal details such as name, mobile number, date of birth, address, gender and place of birth [30], all of which are key components found within a set of fullz.

As illustrated in Table 3.5, the total value of sales across Empire Market for the ID-related category was over $1.8 million accrued across the approximately 2.5 years that the market was active. Compared to the size of the illicit drug market on Empire (total sales value of $265,303,894), the total dollar value of the identity-related market is quite low (0.5% of the total value of sales on Empire). However, cryptomarket sales have previously been estimated to only account for around 0.1% of the total drug market (estimated at US$426-652 billion per annum) [206]. Compounding this, the Global Drug Surveys from the last ten years have illustrated that less than 15% of drug users have used cryptomarkets in the past to purchase

illicit drugs [284-286]. Clearly, most purchases within the illicit drug market are occurring through the more traditional physical marketplaces or alternative online routes of distribution. While admittedly, the illicit drug market is very different due to the nature of its products, given that the cryptomarkets only cover such a small portion of the illicit drug market, the cryptomarkets may be responsible for a similarly small portion of the fraudulent document market.

In fact, it has been illustrated previously that the fraudulent document market spans the breadth of the web, extending digitally beyond the jurisdiction of cryptomarkets and even through to the surface web. These surface web suppliers perform their operations in a range of formats, including storefronts, sellers operating on dedicated forums, email sellers, and vendors who use social media and streaming platforms such as Instagram and YouTube as a means to sell their products [51, 199, 200, 283, 287]. This, combined with being a single market analysis, clearly illustrates that cryptomarkets are not the sole route of access for fraudulent identity documents and stolen personal information, suggesting that the $1.8million figure does not illustrate the entirety of the online fraudulent document market, and that the actual value is likely to be higher. Additionally, given that fraudulent identity documents are known enablers of nearly all forms of serious and organised crime [32], the money (and harm) being generated by their use spans far beyond the criminal environment of document fraud and identity crime.

3.4.2.2 Prices of ID-related products

In general, there has been little research into the prices of fraudulent documents and personal information sold on cryptomarkets, but it has been illustrated that there is a great degree of variation in prices across these cryptomarkets and also across different vendors [47]. In this research, it was found that digital items had a lower average cost compared to physical items across all the ID-related product categories, except for in the ‘Other’ subcategory of the ID

items as illustrated in Table 3.6. This item (price of $1393) was unique within this category, as it was for a copy of the software used by the Department of Motor Vehicles (DMV) to generate licence barcodes.

Table 3.6: The average, median, minimum, and maximum prices for products within the ID sub-category. Prices have been included for both digital and physical products. There were no physical listings for Selfie ID products. For the prices of all products across all categories of the ID-related market, refer to Appendix Table A. 10

		Price (AUD)			
		Average	**Median**	**Minimum**	**Maximum**
Passport	Physical	$9,641	$2,713	$14	$56,828
	Digital	$32	$21	$1	$139
ID pack	Physical	$7,881	$3,623	$29	$22,615
	Digital	$112	$72	$1	$497
Licence	Physical	$578	$258	$21	$5,827
	Digital	$31	$14	$1	$923
ID various	Physical	$863	$716	$15	$4,972
	Digital	$78	$32	$1	$665
Identity card	Physical	$698	$327	$105	$5,608
	Digital	$29	$14	$4	$251
Other	Physical	$36	$32	$4	$1,393
	Digital	$121	$33	$2	$46
Selfie ID bulk	Physical	-	-	-	-
	Digital	$1,582	$989	$325	$3,334

The documents with higher prices are generally those listed as legitimate stolen documents, both with alterations and without, and those documents that come with ‘registration’ in the relevant government databases. The two document types with the highest maximum prices were in the ID pack ($22,615) and passport ($56,828) categories. Both items (along with some of the other more expensive passports) were advertised as legitimate documents that were

stolen or manufactured with the assistance of corrupt officials. They are marketed as a method to "create a new identity". Previous research has illustrated that a fraudulent Australian passport was sold for $35,000 (in 2018) [47], so these prices are not too far outside the realm of possibility when considering the difference in product, general price increases over time, inflation, and increases due to the COVID-19 pandemic, which quite a few sellers specifically mentioned. However, without further information, it is impossible to determine with certainty the motives and reasons behind these higher prices.

3.4.2.3 Types of fraud on Empire

As explained in Chapter 1 Section 1.2.1, there are four main types of document fraud encountered, counterfeits, forgeries, pseudo documents and stolen blanks. According to international data, the fraudulent documents most encountered by police are counterfeits (64%) and forgeries (19%) with the other two types, pseudo documents and stolen blanks, being encountered far less often (<10%) (Keesing ID Academy, 2018 as cited in Baechler, S. 2020 [51]) [175]. From an intelligence perspective, understanding the type of document fraud that is most common within the market can illustrate what document types are most likely in circulation, and provides insight into the M.O. used by those manufacturing fraudulent documents.

Across the 2,425 sales for physical documents, 96% were for counterfeit documents, with the remaining 4% being attributed to the sales for forged documents (Table 3.7). All the listings for forged documents were characterised by phrases such as "legitimate", "authentic", "genuine" and "registered". There were no sales for stolen blank or pseudo documents. After counterfeit licences and identity cards, the most sold document types were in the 'other' category of the various legitimation documents, with approximately $27,000 coming from 290 sales. All documents in this category were counterfeits, and the listing with the most sales (and highest total revenue) was incorrectly described as a 'forged' social security card. Quite a few

documents in the 'other' category were listed as 'forged' items, however, upon closer examination of the listing title or description it was found that the product was in fact a counterfeit document. This illustrated two things; 1) that fraudulent document vendors, and perhaps buyers are either not familiar with document examination terminology, or they are consciously choosing not to use it, and/or 2) that, as mentioned earlier, the descriptions of the products created by vendors are often incorrect, illustrating the need to perform the product classification as described in the method (Section 3.2.3). Across all product types, the highest number of listings were for counterfeit licences (210 listings), and in most cases those items with the most listings also had the most sales, except for the ID various product type.

Table 3.7: Number of sales and listings per fraud type across the ID-related categories. Only physical documents are included here as it was not possible to determine fraud type for the digital documents

		Counterfeit		Forgery (i.e. altered)	
Category	**Product type**	**No. listings**	**No. sales**	**No. listings**	**No. sales**
ID	**ID pack**	5	0	12	0
	ID various	66	7	19	1
	Identity card	72	617	7	1
	Licence	210	1,401	18	75
	Other	1	0	0	0
	Passport	27	17	26	8
Various legitimation documents	**Other**	38	290	15	3
	Statements	1	5	0	0

The M.O. used by the manufacturer of these documents, is not only dictated by their knowledge, techniques and materials available to them [15], but also by what kind of document they are attempting to manufacture. It is unsurprising that so many counterfeit documents are being offered for sale on the cryptomarkets, as the document types with the most sales are largely polycarbonate, credit card style documents that are notoriously difficult to forge due to the integration of tamper proof security features (e.g. licences and identity cards)
[51, 176].

It has been previously found that the most expensive documents are those that have been legitimately issued based on fraudulent information, or forged [47, 200]. This is likely because the forged documents are in most cases legitimate documents that have been stolen, and/or they come with registration within the government or federal database relevant to that document type. In comparison, according to the data examined in this research, the starting (lowest) price for a counterfeit licence is $99.45, while that of a forged licence, in this case a stolen, genuine Italian licence, is $817.50, roughly eight times the price of the counterfeit. A similar trend is noted for the passports, with the cheapest forged passport ($2370.75) still being sold at a higher price point than the most expensive counterfeit passport ($2091.95). These price differences are likely a reflection of the perceived increase in the value, quality, and versatility of forged documents compared to counterfeits, if not just from the vendor perspective, then also from the buyers, given that the prices were considered reasonable enough to complete a purchase. Interestingly, on Empire all sales for forged passports came from one vendor who was supplying both Danish (one sale) and Lithuanian passports (seven sales). All physical Australian documents that were listed and/or sold on Empire were counterfeits, and 90% of the sales for Australian physical documents were for counterfeit licences. Given the format of the Australian licences being credit card style documents that are notoriously difficult to alter (i.e.

forge), this percentage of Australian counterfeit licences within the online marketplace is not surprising.

3.4.3 Geographical considerations and trends

It is common practice within cryptomarket studies to examine trends in relation to country of origin and shipping locations to assist in the identification of trends in the trafficking and movements of illicit goods, along with identifying countries that have a higher concentration of vendors. This can provide insight into where documents and products are coming from, as well as the presence of domestic markets.

3.4.3.1 Document country and origin

While licences seem to be the most popular identity document type sold on Empire and other online markets [51, 269] as well as being one of the most often targeted documents for identity misuse [47], there is often different perceived value, i.e. demand, associated with licences from different countries. Examining the country that a document is claiming to be from can provide some important information about document types that are being targeted by manufacturers, and those that are most popular among buyers. This can indicate trends in document fraud and potentially other types of organised crime within that region. It can also assist in the identification of document types that are more prone to fraud, whether that be due to security weaknesses, or simply a higher perceived value. To facilitate this the 'document country' of the ID-related products listed (on both WHM and Empire), and those sold (on Empire), were examined. It should be noted that the document country is the country that the document is claiming to be from, for example, an Australian passport. Of course, previous research has illustrated that the cryptomarket environment is dominated by users from English-speaking and Western European countries [104, 110, 117, 245, 249], so while the information from this

analysis can assist in identifying the aforementioned trends, this potential bias must be considered.

U.S. products on both Empire and WHM have the highest number of listings with over 40% of each market's ID-related listings devoted to products of this kind (42.8% of Empire, and 40.2% on WHM), consistent with previous research [202]. The difference in the number of listings between the U.S., and the next most listed document country, Australia, is stark. While Australian documents are the second most listed type, these products account for only 7% of the listings on both Empire and WHM. Following closely behind Australia is the U.K., Canada, and France. When considering the number of sales, the U.S. again dominate the market, followed by Australia, U.K., Canada, and France (Figure 3-9). The volume of both sales and listings for U.S. documents and stolen personal information (the identity fraud-related category), is higher when compared to the other document countries (Table 3.8)

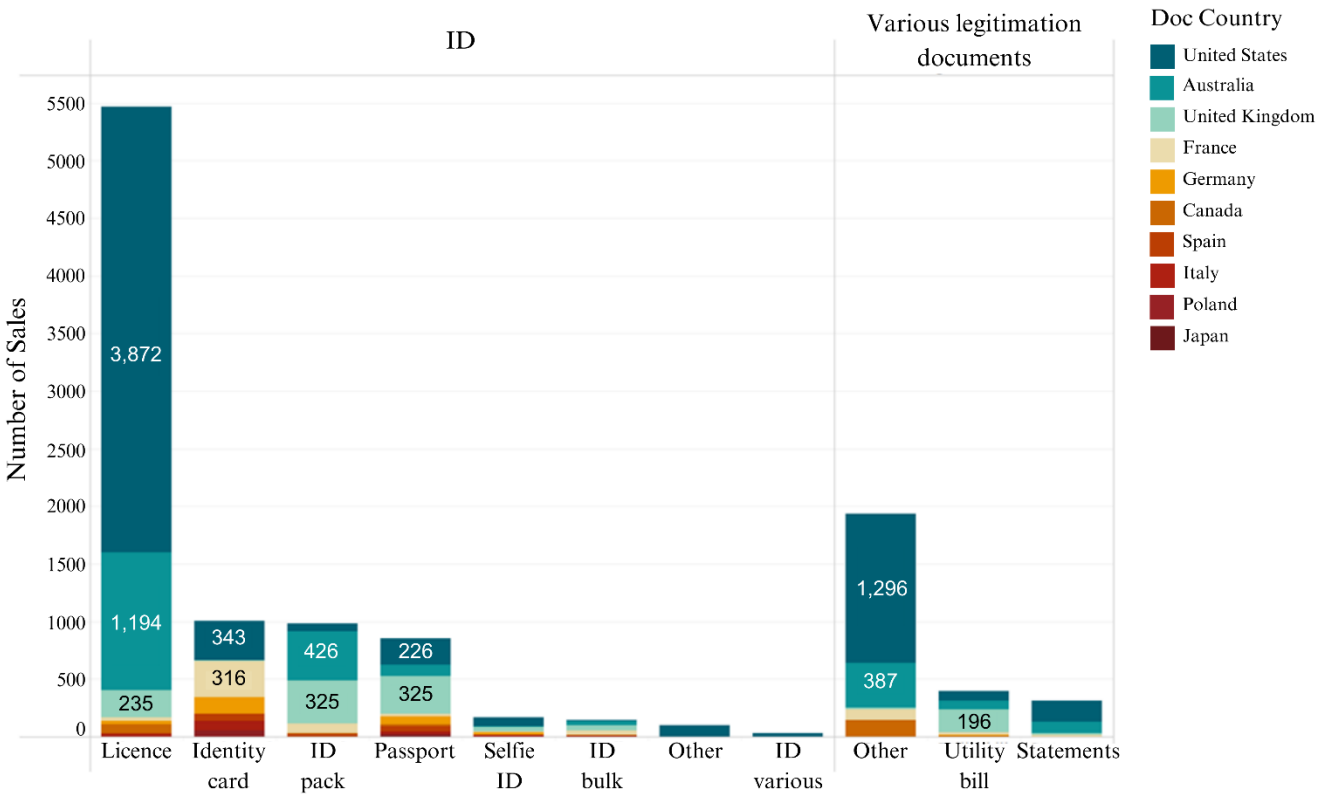


Figure 3-9: The number of sales per document type, with the colour indicating the document country. Only the top ten document countries (regarding sales) have been included. The identity fraud related category is not shown here as it obscured the other categories and was largely just dominated by the U.S. products.

Table 3.8: Number of sales for each document country across the three ID-related subcategories, and the total sales (%). Only the top five document countries (number of sales) are illustrated here.

	Number of Sales				
Document Country	*ID*	*Identity fraud*	*Various legit.*	*Total*	**% of ID market**
U.S.	4,719	25,353	1,553	31,625	65%
Australia	1,764	595	570	2,929	6%
U.K.	1,023	877	219	2,119	4%
Canada	98	443	149	690	1%
France	487	2	136	625	1%

While this agrees with other dark web market analyses, such as that conducted by Baravalle et al. [202] other work conducted by Holt and Lee found in their analysis of the broader online document market that the most commonly listed documents were for those from European (EU) member states (51.2%), followed by Asian (11.7%), South American (8.4%) and Southwest Asian and North African (SWANA)[22] (7.2%) nations [200], with Australian/New Zealand documents only accounting for 3.6% of the products listed [200]. This is again contrasting to previous research which indicated Australian documents to be some of the most encountered products on the dark web [51, 199, 269]. Of course, the work conducted by Holt and Lee examined vendors across the open and dark web, and did not solely examine the cryptomarket facilitated trade, suggesting that there may be some distinction between the products offered and sold based on the type of shop front the vendor is operating.

Over the last few years, identity crime has continued to rise on an international scale [30, 288]. During the operation of Empire and WHM (between 2019 and 2021), there was a noted increase in the instance of identity crime in the U.S., with the number of complaints and total losses nearly doubling between 2018 and 2021 to 847,376 complaints and $6.9billion USD respectively [288]. The more specific crime types of identity theft and personal data breaches, being those most closely linked to the products within the identity fraud category, also experienced increases in the number of complaints and total losses across these three years, with the U.S. having the highest number of victims in 2021, followed by the U.K. and Canada [288]. The prevalence of the victimisation of those individuals from the U.S. was further exemplified by a 2018 study that examined the cybersecurity behaviour of 6,000 working professionals across the U.S., Australia, France, Germany, Italy, and the U.K. This work

[22] The commonly used term ‘Middle East’ is an outdated colonial term used to describe the location of Southwest Asia and North Africa in relation to Europe and the West. The term Southwest Asia and North Africa (SWANA) is used instead.

revealed that 33% of U.S. respondents had experienced identity theft, which was twice the global average [289].

Given the victimisation rate of identity crime within the U.S. [288, 289], it starts to make more sense why U.S. products are so prevalent on these cryptomarkets. It should be noted however, that both the FBI and the cybersecurity company that conducted the studies mentioned above are U.S.-based, so there may be some unintentional bias as they are more likely to have access to a higher number of reports from U.S. citizens [288, 289]. Compounding this is the often over-representation of U.S. users, both vendors and buyers, on English-speaking cryptomarkets [104, 110, 117, 249] and their much higher population, which may be contributing to the higher occurrence of U.S. documents on these markets. However, this does not discount the potential for these results and those from the FBI [288] and the previous study [289] to be highlighting a potential trend between identity crime and the online ID-related market.

Australia, France, and Canada have a high percentage of their product types within the various legitimation category (19%, 22% and 22% respectively), compared to the U.S. and the U.K. which have 10% or less. We can see that Australia has a high number of sales in the various legitimation category when compared to the identity fraud category, as does France. Utility bills, bank statements, and other similar document types have a well-established role in proving an individual's identity in Australia, with them being crucial parts of satisfying the 100-point identity threshold which was introduced in Australia to reduce instances of financial fraud [47]. To prove their identity the individual must supply a range of documents, all of varying degrees of security (and therefore different point values) [47]. This threshold must be met to gain access to identity documents such as driver licences and passports, but also to rent a property, open a bank account, and access government benefits such as Centrelink. Similarly, in France, these various legitimation documents are required to serve as a *justicatif de domicile* (proof of physical address). Even though most of the state issued ID cards have the address printed on

the back, a utility bill, bank statement or the like (that is less than one year old) is required as a proof of address [290].

Origin country

When looking at the country of origin for the ID-related market, unsurprisingly, the U.S. is still the most common, followed by Australia and the U.K. These three countries are supplying most of the products within this market, with 37% of the listings (1694) and 29% of the sales (13,591) being shipped from these countries of origin. This suggests that Australia may potentially have a more prominent role within the document market when compared to the overall cryptomarket criminal environment. In the overall markets for both Empire and WHM the five main contributing countries for vendors and sales were, in order, the U.S., the U.K., Germany, the Netherlands and then Australia (Appendix Figure A. 6). While the prevalence of these origin countries is not surprising, as English speaking and Western European countries do exhibit dominance within the English language cryptomarkets [117, 249], particularly in relation to the illicit drug market, it is interesting to see the position of Australian based vendors within the ID-related market. However, it must be remembered that the study of these two marketplaces, and therefore the results presented here are not representative of the entire market and simply provide an indication of the market environment on these two cryptomarkets.

As shown in Figure 3-10 the five countries that are contributing the most sales within the ID-related market are the U.S., U.K., Australia, Canada and Germany. When examining the types of ID-related products these countries offer, there is quite a bit of variation. Most listings and sales from the U.S., U.K. and Canada are for fullz and identity fraud packs. Contrastingly, the vendors based in Australia almost exclusively list and sell products that fall within the ID category, with a much smaller proportion of sales within the identity fraud category, consistent

with the trends noticed in Table 3.8. This of course is not considering those listings or sales that had an origin country of Worldwide.

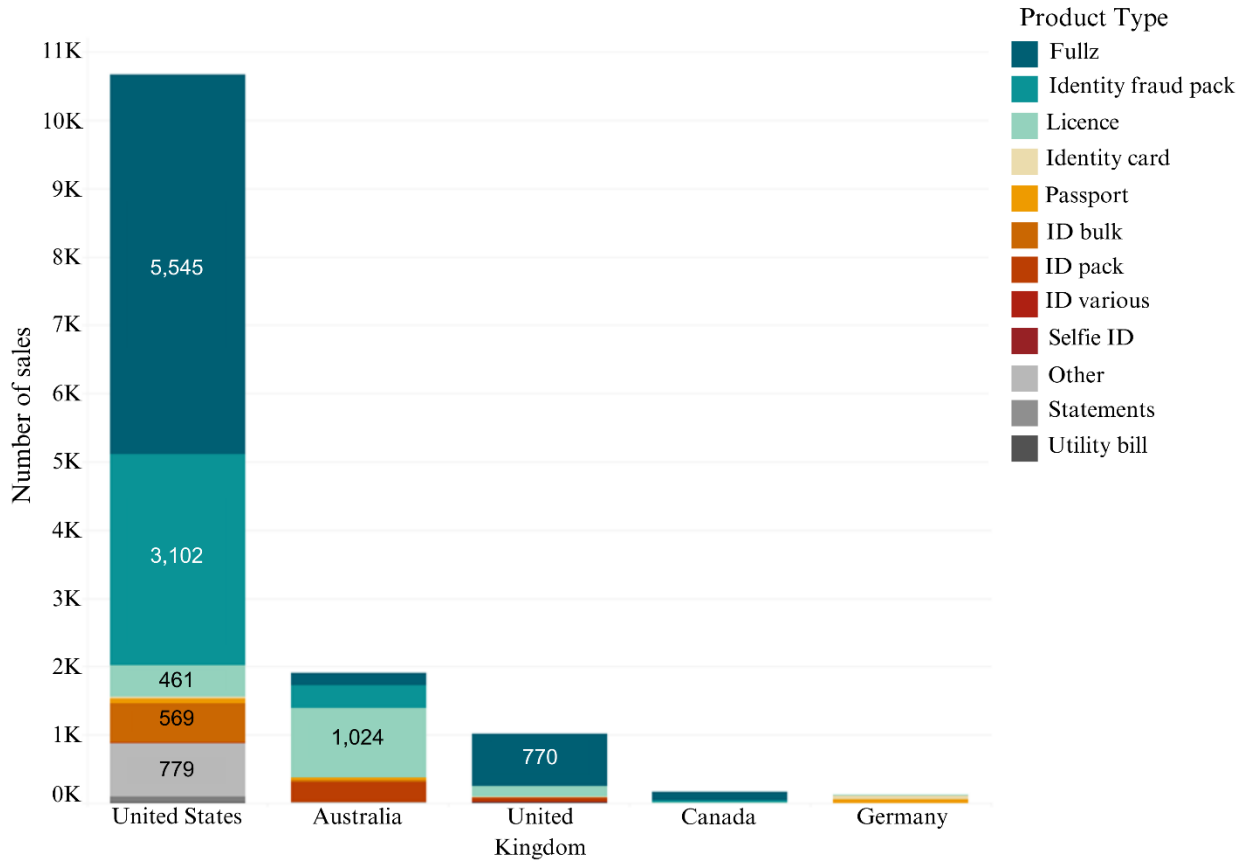


Figure 3-10: Number of sales per origin country (top five regarding number of sales). The colour indicates the product type as indicated in the legend.

Interestingly, when examining the origin and document countries, a significant portion of the sales for U.S. (95.7%), Australian (89%), and U.K. (93.2%) documents were being shipped from vendors originating from within the respective country, suggesting a potential correlation between origin country and the types of documents being offered by vendors (Figure 3-11). In fact, most origin countries supply domestic documents (i.e. documents claiming to be from that origin country), with this trend continuing in the Canadian, French, German and Polish documents. While the vendors originating from the U.S. have some sales for listings that were classified as 'Not Specified' and 'Various' in relation to document country, Australian and U.K. vendors have sales almost entirely for domestic documents, aside from two sales from an

Australian vendor for a Spanish document. A parallel could be drawn between the document market and the illicit drug market in relation to product specialties being dictated by domestic access or familiarity with the items listed, impacted by the origin country of the vendor [110]. Furthermore, selling items within the vendors country of origin reduces their risk of being detected, with most mail controls and checks being conducted at the borders by customs [104, 110].

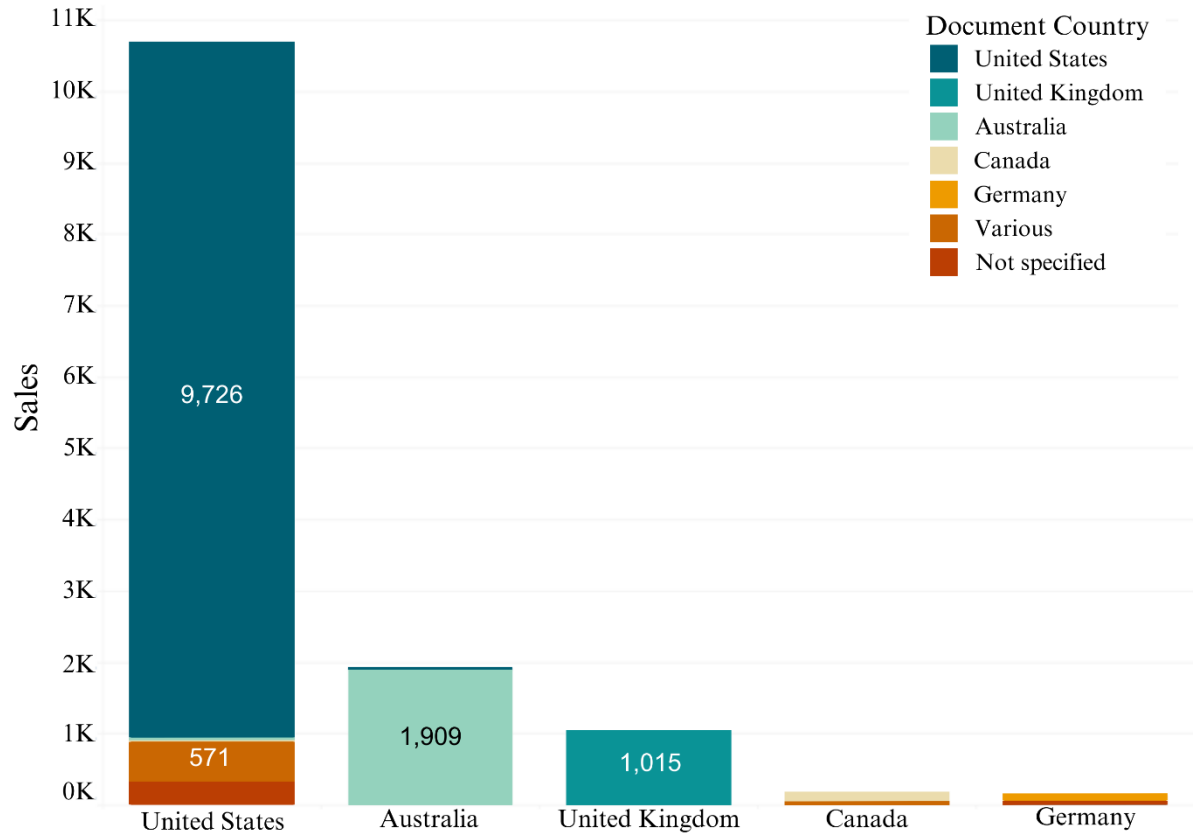


Figure 3-11: Number of sales per origin country (ship from) with the colour indicating the document country of the products

3.4.3.2 Trafficking patterns

A key component of understanding the illicit marketplace is using the shipping information provided by the vendor, to not only infer their country of origin, but to also provide an indication of the movement of goods. While the figures above (Figure 3-10 and Figure 3-11)

illustrate the country of origin in isolation, revealing the most popular product categories from each country, a combined analysis of the origin and destination countries allows the identification of market types i.e. domestic or international. This can assist in illustrating the behaviour of vendors and buyers, providing an indication of the extent of the market within each country [117].

As outlined in the Materials and Methods (Section 3.2.4.3) all digital products were removed from the analysis of the trafficking patterns, as well as any listings that had both the origin and destination country listed as Worldwide. This left 189 listings and 552 sales from Empire to examine, and 323 listings from WHM. Figure 3-12 and Figure 3-13 illustrate the trafficking patterns for both WHM and Empire, illustrated through the frequency of the origin and destination country combinations in the product listings, and in the number of sales on Empire (Figure 3-13 right). Because of the prevalence of digital products, the results presented here are not representative of the entire marketplace, as the vast majority of listings and sales across both WHM and Empire were for digital products. This analysis just provides some insight into the movement of the physical goods in the marketplace and can only provide an indication of where these products may be originating from.

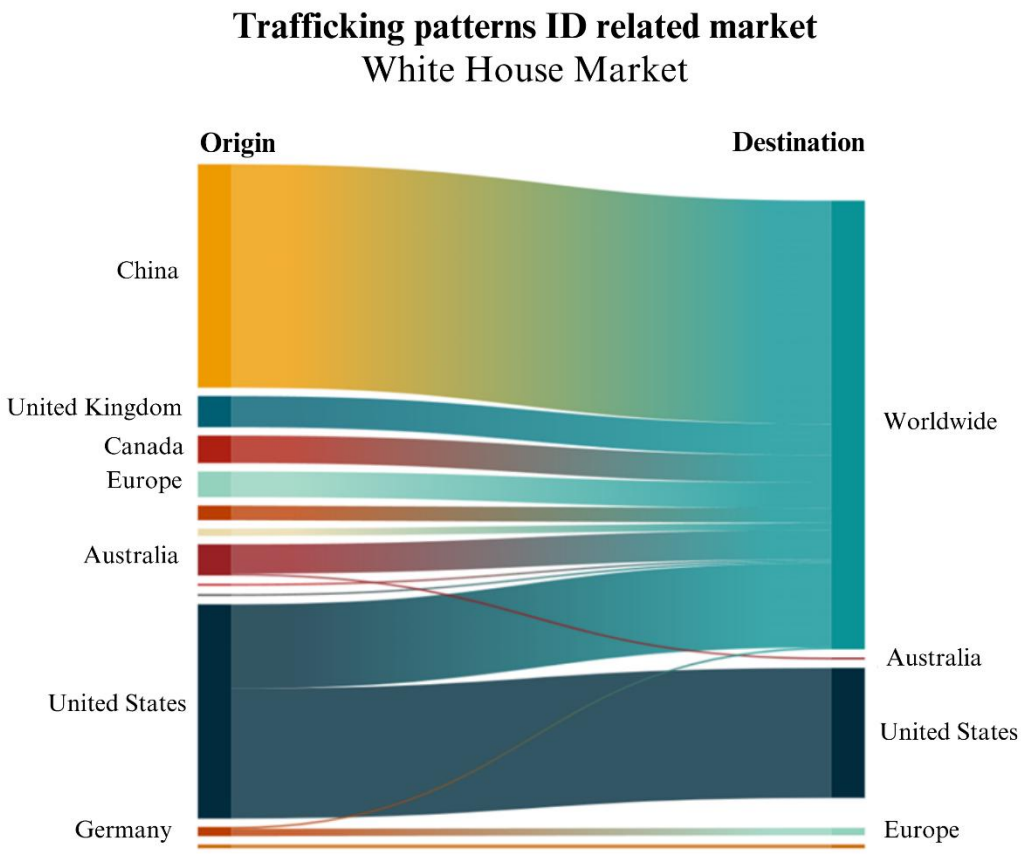


Figure 3-12: Sankey Alluvial diagrams illustrating the movement of ID-related goods across WHM from their origin to destination countries. The colours have been kept consistent across figures 3.12 and 3.13 to make comparisons easier.

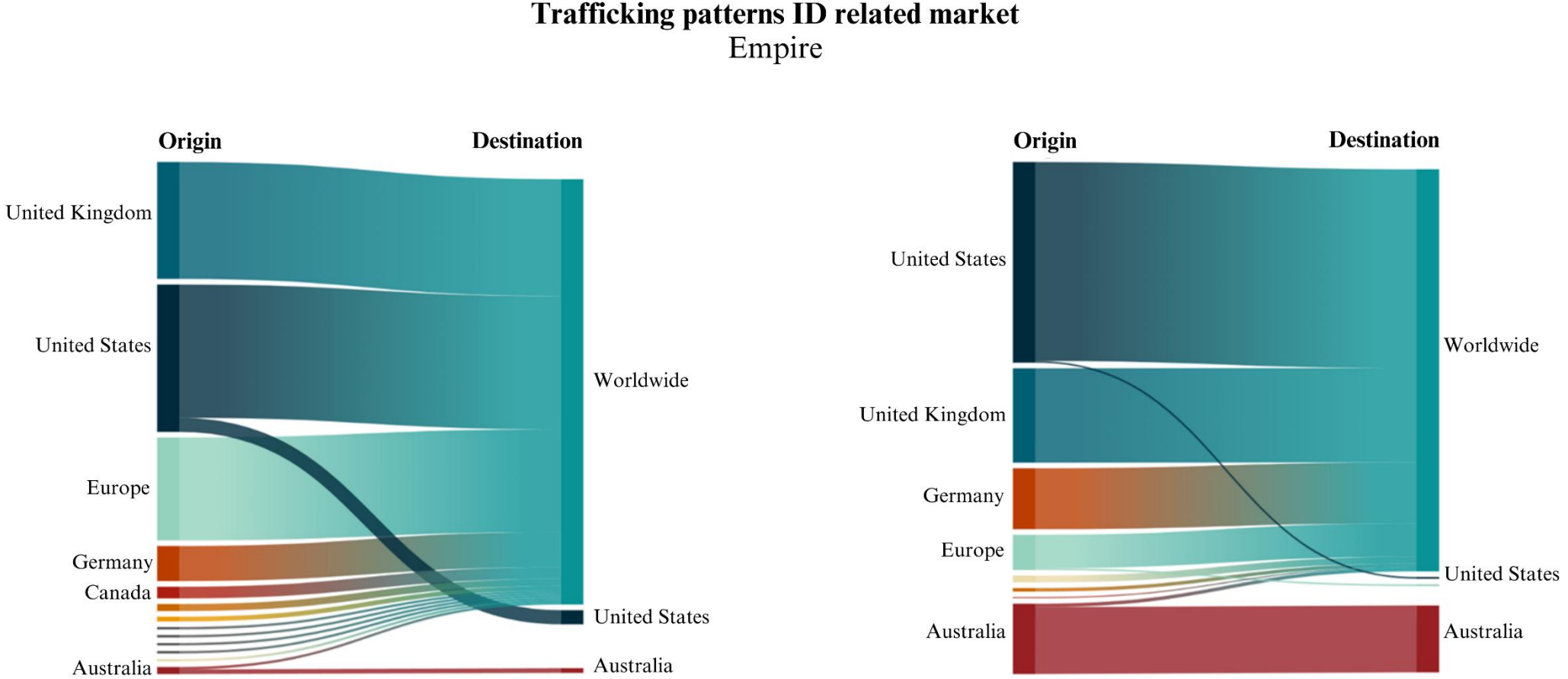


Figure 3-13: Sankey Alluvial grid illustrating the movement of ID-related goods from their origin to destination countries on Empire. The diagram on the left has been created using the number of listings on Empire, whereas that on the right has been created using the number of sales per origin and destination combination. The colours have been kept consistent across figures 3.12 and 3.13 to make comparisons easier.

Across the ID-related listings, most vendors indicated that they would ship items worldwide (91% on Empire and 76% on WHM), with a much smaller proportion of documents being shipped to the U.S., Europe, and Australia. One interesting distinction between WHM and Empire, is that within the ID-related market most of the ID-related products on WHM are shipping from China and the U.S., while Empire has very few products coming from China, with the U.S., U.K., and Europe being the most prominent origin countries. WHM also had a much higher number of listings being shipped to the U.S., 21% compared to Empire's 3.5%.

The shipping information for the ID-related products, both listings and sales, suggest there may be a domestic market within both the U.S. and Australia, much like what was seen when looking at the trafficking trends for the overall market (Appendix Figure A. 7 and Figure A. 8). However, when looking at the shipping information based on number of sales on Empire (Figure 3.13, right) contrasting to the U.S. (two sales), the domestic market in Australia (78 sales) is more prominent. According to this trafficking analysis, the WHM and Empire specific portion of the cryptomarket facilitated online market for physical Australian documents may potentially be originating from domestic vendors. While there is a domestic portion of the market, much like in the illicit drug [96, 104, 110, 117], and overall market, it is unlikely that there are no international vendors willing to ship ID-related products to Australia. This is an illustration of how the size of this analysis, the number of listings and sales examined is a limitation, and that the analysis of trafficking patterns for the fraudulent document market on Empire and WHM can only suggest potential origins of interest and does not capture the entire market for physical fraudulent documents.

Given the popularity of Australian documents on Empire and WHM, the listings for Australian documents were more closely examined to see what countries they were originating from and

what vendors were supplying them. Within the ID-related market across Empire and WHM combined, there were 294 listings for Australian documents, 27 of which were listings for physical documents (seven were removed as their origin country was 'Worldwide') which were being supplied by nine different vendors. Most of the listings for these Australian documents had Australia as the country of origin, with China and U.S. following behind (Figure 3-14). Similarly, when looking at the number of sales, the potential domestic nature of the Australian document market is suggested with 89% of sales having an origin of Australia, with the other 11% coming from the U.S. While this potential Australian domestic market is consistent with what was found in Figure 3-12 and Figure 3-13 it is possible that there are Australian documents being manufactured in and shipped from other countries (including the U.S. and China). In both cases, the listings from these two countries indicated 'Worldwide' as the destination country, meaning it is possible that they would be shipped to Australia. Of course, this is not considering those documents being shipped from 'Worldwide', so there are likely other countries contributing to the Australian document market, but from this analysis, it was not possible to identity them.

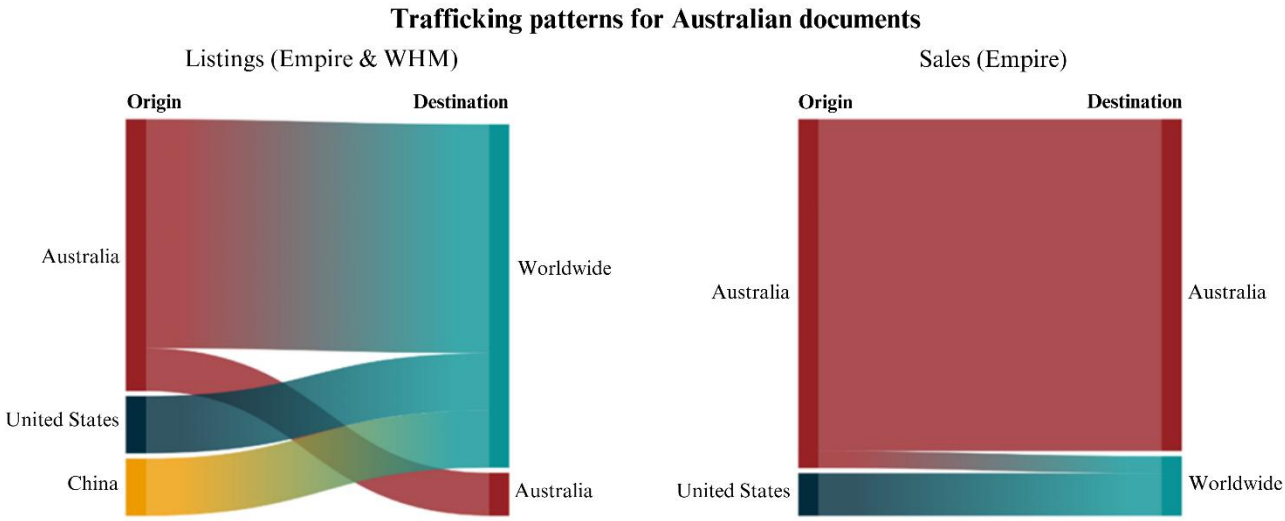


Figure 3-14: Trafficking patterns for Australian documents across both Empire and WHM. Listings are on the left, with the number of sales (Empire) on the right.

Vendors are, naturally, risk averse, and shipping packages of illicit goods to countries with higher border controls exposes them to increased risk of package interception, resulting in potential arrests, or increased negative feedback from the buyers when the package does not arrive [104, 110, 117, 249]. When looking specifically at the trade environment in Australia, the domestic market for illicit drugs has also been attributed to the geographic isolation of Australia, the presence of domestic manufacturing, and the high domestic prices [104, 110].

Undoubtedly, the geographic isolation of Australia plays a role in the trafficking of any physical illicit goods, combined with the general risk-averse nature of vendors leading them to avoid shipping to countries with strict border controls. However, it is impossible to say with certainty how much these factors are impacting the shipping of fraudulent documents based solely on the limited analysis of two markets. Figure 3-14 does suggest that there is domestic

shipping, with the majority of the Australian documents on WHM and Empire originating domestically, and while there have been previous instances of domestic manufacture of these documents [47, 192, 291], it is not possible to say, at this stage, to what extent this manufacture is occurring. When considering the other potential factors that may be impacting the presence of this domestic market, it is unlikely that prices are significantly impacting the market, especially considering the mostly low prices due to the dominance of digital products. So, until more concrete conclusions can be made regarding the domestic manufacturing of Australian documents, the most logical conclusion is that the geographical isolation and strict border controls of Australia, combined with the risk-averse nature of cryptomarket users is the most likely reason for a low rate of international shipping, and a stronger domestic market. It must, of course, be remembered that the entire fraudulent document market is not represented on Empire and WHM with the market existing across all levels of the web [200, 269]. So, this analysis of the cryptomarkets is just one part of a much bigger puzzle.

3.4.4 Vendor username comparisons

Beyond the well documented reactive movements of vendors after a market closure, it is possible that vendors are operating profiles on multiple marketplaces, either as a risk mitigation tactic [236], a backup should their main market of choice close, or simply to expand their reach and therefore increase their likelihood of higher profits [239, 277]. While intrinsically difficult to identify the motive behind the diversification, and whether it is prompted by external forces, the comparison of usernames and PGP keys across markets can provide an idea of the proportion of vendors that are diversifying, thus assisting in the identification of prolific offenders.

Beyond identifying connections between vendor usernames across different markets, the comparison of PGP keys within a single marketplace can also assist in the identification of vendor accounts that are operated by a single criminal network or organisation [203]. When comparing all the PGP keys across the usernames on Empire, forty (1.4%) were found to share a PGP key with at least one other username, most in pairs or groups of three. While the majority of vendor usernames across Empire were only associated with one PGP key, consistent with previous research [203], Empire did show a higher level of connectedness between the vendors compared to WHM where only six (0.2%) vendor usernames were connected by the same PGP key. This degree of connection between vendor usernames was not present within the ID-related market. There was just one username (Vendor SP) from the ID-related market on Empire that shared a PGP key with a username (Vendor BD) within the overall market. Interestingly, Vendor SP and Vendor BD were offering varied products, with each username having a speciality, being ID-related products and fraud-related products respectively. This trend of specialising based on usernames was noted for all PGP key pairs across the overall markets of Empire and WHM.

The usernames and PGP keys were then compared across both markets to identify those ID-related vendors that were operating across both WHM and Empire. In the username comparison, only those usernames that were found to be identical (ignoring capitalisation) were considered to be the same. Out of the total 318 ID-related vendors across both markets, 50 usernames (18%) were consistent across both markets, and 58 PGP keys were linked. 22 vendors were identified as being significant contributors to the online illicit marketplace for fraudulent documents (those that were identified as the ten vendors contributing either the highest number of listings or highest number of sales) and out of those 22 vendors, 18 had usernames that appeared on both Empire and WHM. In fact, all the vendor usernames identified

in the top ten regarding the number of sales on Empire were also present on WHM. It is possible to hypothesise that these 22 vendors may potentially have a large impact on the overall document fraud market on Empire, and given their presence on WHM, they may be exhibiting similar patterns of behaviour on this other market.

Connolly et al. 2023 examined the usernames of vendors across four different cryptomarkets, Darkode, Tor2door, Bohemia and ViceCity [292]. In their work, they did not anonymise the vendor usernames, which facilitated a comparison between their figures and the vendor usernames present in WHM and Empire (which have been anonymised in this research). Table 3.9 shows the eleven vendors that were examined by Connolly et al., and the 'x' indicates their presence in the respective market. We can see that a total of nine vendor usernames were present across at least two markets, with the most interesting being the four vendor usernames present within the ID-related markets on WHM and Empire, indicated in cream. In fact, Vendor G was the vendor on Empire with the second highest number of listings and sales in the ID-related market, illustrating the extensive activities of this username/vendor.

Table 3.9: Username (proxy for vendor) presence across multiple markets. Adapted from Connolly et al. [289] and added to from this research data (Empire and White House Market). All vendor usernames have been anonymised. Those Empire and WHM vendors shaded in cream appeared within the ID-related markets

Vendor (anon)	Empire	WHM	Darkode	Tor2dor	Bohemia	ViceCity
Vendor S	x	x	x	x	x	x
Vendor K	-	-	x	x	x	x
Vendor R	x	x	x	x	x	-
Vendor M	x	-	x	x	x	-
Vendor G	x	x	x	x	x	x
Vendor P	-	x	x	-	x	x
Vendor D	x	x	-	x	x	x
Vendor G2	x	x	x	x	x	x
Vendor D2	-	-	-	-	x	-
Vendor K	-	x	x	x	x	-
Vendor B	-	x	-	-	x	-

The percentage of linked vendors, in both the ID-related and overall markets (18% in both cases), is not surprising considering that both markets were contemporaries. Compounding this, after the sudden exit scam of Empire [293], WHM was one of the main markets that was still active, allowing it to partially fill the void created by the closure of Empire. It is commonly accepted that when a top-level market closes, vendors will migrate to competing markets [218, 220, 221]. In 2017 Moeller et al. quoted a user on a Darknet news forum who was commenting on the "herd-like nature" of the darknet market user base: "If Silk Road is down, everyone moves to Agora, if Agora is down everyone moves to Evo…and so on…[…] the DNM's user base is very herd-like" (DeepDotWeb interview) [109]. Despite this, the proportion of the market that performs this reactionary migration is smaller than anticipated, especially when compared to what was noted for Empire and WHM. Decary-Hetu et al. illustrated that following Operation Onymous, only 8% of active vendors moved their activities to Agora or

Evolution [220]. Furthermore, Ouellet et al. in 2022 illustrated in their analysis of seventeen marketplaces before and after the seizure of DarkMarket (another large marketplace during its operation) that the interconnectedness of the cryptomarket ecosystem only increased by 10% [236]. Even considering the limitations that these percentages do not include those vendors that changed usernames, moved to physical markets, or simply moved to markets other than Agora or Evolution, this is a much smaller percentage than would be expected given previous research [218, 220, 221], the overlap identified in this research, and the general discussion on forums regarding the movement to new markets.

Of course, this reactionary migration is not the sole motivator for market diversification, with recent research indicating that many vendors sell their goods across multiple marketplaces, [220, 226, 239, 277, 294], with numbers increasing in recent years [239]. This practice is so common, that many market administrators encourage and facilitate the diversification of vendors, offering to waive vendor bonds (the cost for a vendor to register on a market) based on that vendor's presence on other apex markets [236]. One vendor described in Ouellet et al, 2022, how they were 'grandfathered'[23] into White House Market, after which they had their vendor bond waived for almost every other marketplace [236]. Indeed, the slightly higher percentage of linked usernames and PGP keys on WHM and Empire may be indicating an increase in the vendors diversifying their activities for non-reactionary reasons. However, the crawling on Empire in this analysis was done just prior to the markets exit scam and closure, so this inflated percentage of cross-market vendors may be indicative of increased vendor movements due to the impending closure. While exit-scams are in most cases a surprise to users, there are occasionally signs that may hint at an impending scam or closure such as

[23] To exempt someone or something from a regulation or law that has recently been implemented

delayed admin responses, as well as market links, mirrors[24], and/or landing pages not functioning [295] all of which are usually discussed on the dark web forums such as Dread[25] [295, 296].

Overall, while 18% of the ID-related vendors across these markets have seemingly diversified their activities, most of the ID-related vendors within Empire and WHM are operating on a singular market, which is in line with previous research [203]. However, this is based solely on the examination of just two marketplaces, so it is entirely possible that these vendors are simply diversifying to different marketplaces than those examined here. Furthermore, it is not possible to account for vendors that may choose to operate under multiple usernames and/or PGP keys. There have also been instances of username theft, where individuals may take the username of a successful vendor and register it on other markets, offering it to the original user for a price, or simply trying to bulk out their own business based on the reputation of the previous vendor. There were quite a few vendors on Empire that included disclaimers, outlining their old usernames on previous markets, and that they are not affiliated with the username on this market, that it is being operated by a different vendor.

What this indicates is that the ID-related vendors are exhibiting the same characteristics of diversifying (to increase market presence and profits) and displacing their activities in the face of market closures, features that have been noted in cryptomarket vendors in general [218, 220, 221]. The presence of the most prolific vendors (being those with the highest number of sales, listings and overall profits) across multiple markets, including those examined here and by Connolly et al. [292] indicates that the cryptomarket-facilitated online market for ID-related

[24] A "mirror" is used to refer to a version of the marketplace that is hosted on a different onion address (Tor) or on other networks such as i2P or Freenet [288].
[25] In operation since 2018, Dread is a dark web forum, like Reddit, that includes discussions and news focussed on dark web markets [296].

products is punctuated by prolific offenders that are significantly contributing to this criminal environment, both that of identity crime and document fraud, and the general cryptomarket ecosystem.

Furthermore, the presence of these vendors across multiple markets highlights that the costs of the ID-related market estimated in Section 3.3.2.1 are most definitely an underestimation. Because this online market is spread not only across numerous dark web markets but also across all levels of the web as identified by Holt and Lee [200] and Romagna [199], the costs and damages associated with this market are likely far higher than illustrated by any one study. However, the fact that vendor usernames and PGP keys are being used across different markets, does support that the neutralisation of even one prolific ID-related vendor could reduce the number of ID-related items that are being traded in the online markets.

3.4.5 Australian documents in the cryptomarkets

Across both Empire and WHM combined, there were 294 listings for Australian documents controlled by 52 vendors, totalling 7.0% of the document market. On Empire, there were 2,929 sales for Australian documents from 31 vendors, which was 6.0% of the sales for ID-related products, with a total sales revenue of $183,557. Overall, within the Australian market, driver licences, and identity (ID) packs were the products with the most sales. This prevalence of Australian documents within the online document market is not anomalous to these two markets, with it being mentioned in previous research [51, 269]. The popularity of Australian driver licences can likely be attributed to the valuable personal information that they contain (as mentioned earlier), but also perhaps due to their ability to be used as ‘gateway documents’. These documents can be used in combination with other lower security documents, such as utility bills, to satisfy the 100-point identity threshold, thus serving as proof of identity and

enabling the user to fraudulently gain access to more secure, legitimate, documents, such as passports. From a product perspective, on Empire market, this 100-point pack (or 'digital wallet') often included a scan of a driver licence, credit card, bank statement, and/or utility bill. The prevalence of this identity check system may very well be another reason why Australian driver licences and particularly Australian ID packs are so popular, with Australian ID packs having the highest number of sales compared to all other document countries. The popularity of Australian driver licences also exists beyond the cryptomarket ecosystem, with driver licences being the most misused document as reported by victims of identity crime in 2017, 2019, 2020 and 2023 [30, 31, 47].

3.4.5.1 Australian document prices

The prices of fraudulent Australian identity documents on cryptomarkets are not widely published, with the most recent information published by Jorna et al. in 2017 [47] using data that they collected from a range of Australian police forces, and government organisations. The results from this work have been combined with information gathered from WHM and Empire to create Table 3.10.

Table 3.10: Comparison of the price ranges for Australian Identity Credentials available on the digital illicit marketplace. The information from 2015 and 2018 was adapted from [47]. Note Not Sold indicates that the item was not sold during the data collection/crawling periods and was therefore not captured in the data examined.*

Australian identification credential	**2015**	**2018**	**2020 (Empire)**	**2020 (White House Market)**
Driver licence (physical)	$417 - $450	Not sold*	$100 - $263	$258 - $724
Driver licence (digital)	$75 - $750	$12 - $20	$7 - $82	$13 - $30
Passport (real)	$5,110	$2,000 - $3,000	Not sold*	Not sold*
Passport (digital)	Data not available	$10 - $50	$8 - $138	$8 - $126
ID pack	$1,170	$500	$1 - $1014	$19 - $472
Utility bill	$57	$20	$7 - $30	$10 - $30
Statements	Data not available	$23 - $50	$7 - $42	$20 - $50
Selfie ID (digital)	Data not available	Data not available	$71 - $258	Not sold
ID bulk (digital)	Data not available	Data not available	$31 - $409	$30 - $100

Since 2015, there have been some noted price fluctuations, as illustrated in Table 3.10. Some new product types that were not available in the data collection for 2015 and 2018 were the digital ID packs, ID bulk, and Selfie ID. While this seems to support the theory that Selfie ID

as a document type only started appearing in 2020 [201], it is possible that this document type simply wasn't captured in the previous research. Unfortunately, there were no listings present for any Australian passports (physical) on either Empire or WHM. This is not surprising as successfully counterfeited Australian passports are apparently uncommon and not often encountered by border patrols [297]. This is one of the potential reasons why these products are less prominent on the illicit marketplace, and why previous research has illustrated that in some instances, prices can reach around $35,000 for an unaltered stolen Australian passport [47].

The prices of fraudulent identity credentials have been shown to fluctuate according to supply and demand. In 2018, IDCARE [47, 298] suggested that the price differences between 2015 and 2018 were likely due to a spate of significant data breaches, resulting in supply exceeding the demand for the products. Unfortunately, while it is not possible to draw comparisons to the number of data breaches in the years preceding 2018, it is interesting to note that while the number of data breaches has been gradually increasing each year, the prices of the Australian fraudulent credentials has also started to increase again since 2018 (Table 3.10), with some price differences even occurring between Empire and WHM. This is seemingly contradicting the hypothesis in previous research regarding supply and demand influences from data breaches.

While the number of data breaches occurring has been increasing since 2018, [299-302], what has been noticed, and is consistent across both WHM and Empire, is that the Australian cryptomarket facilitated document market seems to be quite specialised and is not overly populated by vendors, with only 37 vendors listing Australian documents across Empire and WHM combined. This is illustrating that while there may be an increased number of data

breaches occurring, because the Australian document market is only populated with a small number of vendors, the supply to the market is somewhat controlled, and therefore so are the prices. When examining the markets data it was noted that many vendors across the market made specific note of increasing their prices due to COVID-19 as the pandemic had made it harder to source product and ship items. So, this may be also having an impact on the variation in the prices.

3.4.5.2 Vendors selling Australian documents

When looking at the vendor behaviour across the listings for the Australian documents on the markets' (Figure 3-15), most vendors have diversified quite broadly across the different product types. As an example, one of the ten vendors with the highest number of listings, has items appearing in all three of the ID-related subcategories across both Empire and WHM. Given that most of the items listed in the marketplace are digital (87% of listings in the Australian document market), it makes sense that vendors are for the most part, broadly diversifying, as the skill set required to sell the digital templates and scans, is not as specialised as the manufacture of physical counterfeit documents.

Contrasting with Figure 3-15, the sales across Empire are much more concentrated (Figure 3-16), with most of the sales being contributed by only a few vendors, with less diversification in the product types sold. Figure 3-16 illustrates the number of sales per document type, with each colour indicating a different seller. Of the 2,929 sales for Australian documents on Empire, 2,752 of them (94%) were for digital documents, with all remaining sales being for counterfeit physical documents, most of which were driver licences. Overall, considering both physical and digital documents, 40.8% of the sales for Australian documents were for driver

licences, followed by ID packs (14.5%) and identity fraud packs (13.2%) and 'other' from the various legitimation category (13.2%). All other document types fell below 10% of the sales.

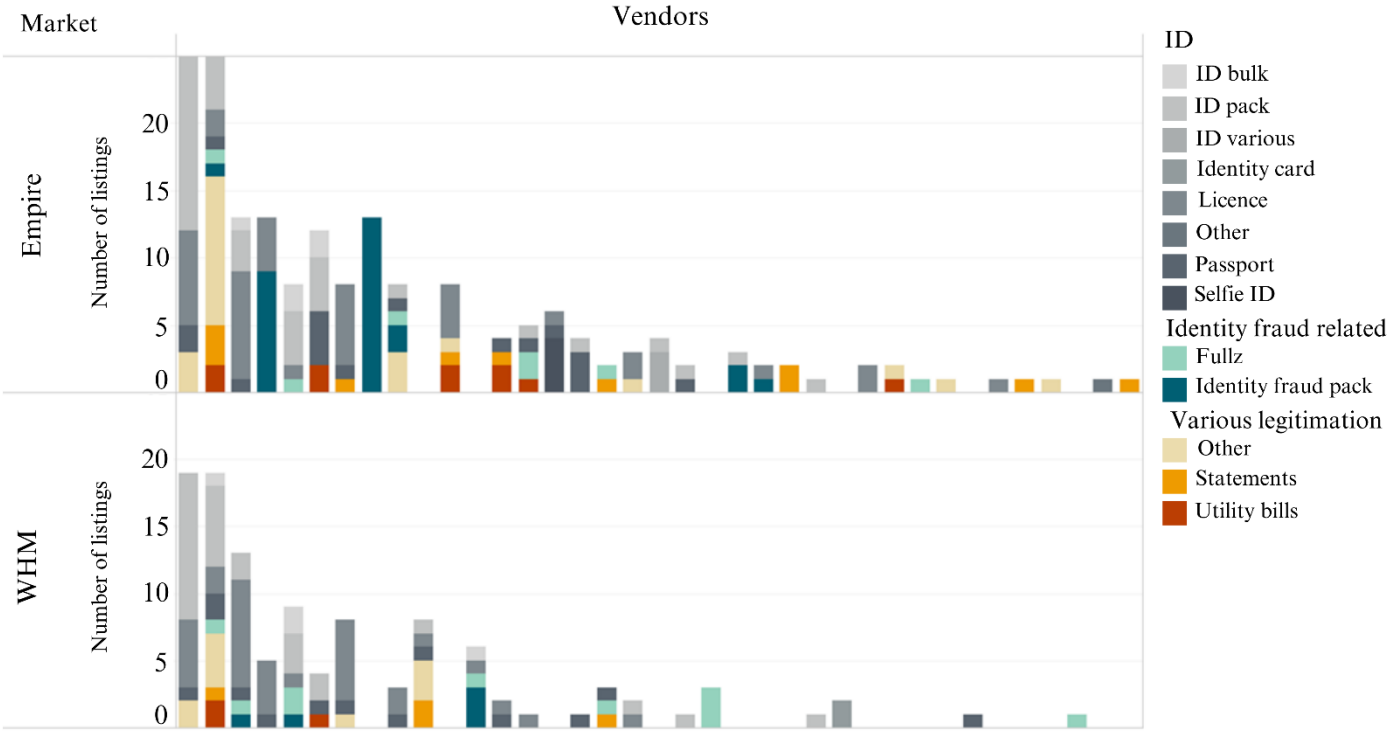


Figure 3-15: The number of listings per vendor (Australian documents) across Empire and WHM with the colour indicating the document type and category. Every vendor is depicted as a column along the horizontal axis.

As discussed previously, to properly identify those vendors that are playing a significant role in the illicit marketplace, the number of listings, sales, and the total sales revenue should be considered to ensure that those vendors that are making the largest contributions to the market are being identified. While the ID-related market for Australian documents is quite small (6% of the ID-related sales), the three main vendors are contributing 1,901 sales to the market, which is 65% of the sales for Australian documents. This suggests that the cryptomarket facilitated portion of the online market for Australian fraudulent identity documents may be

punctuated by prolific offenders, much like what has been noted in the physical market (Chapter 2 Section 2.3.2.1).

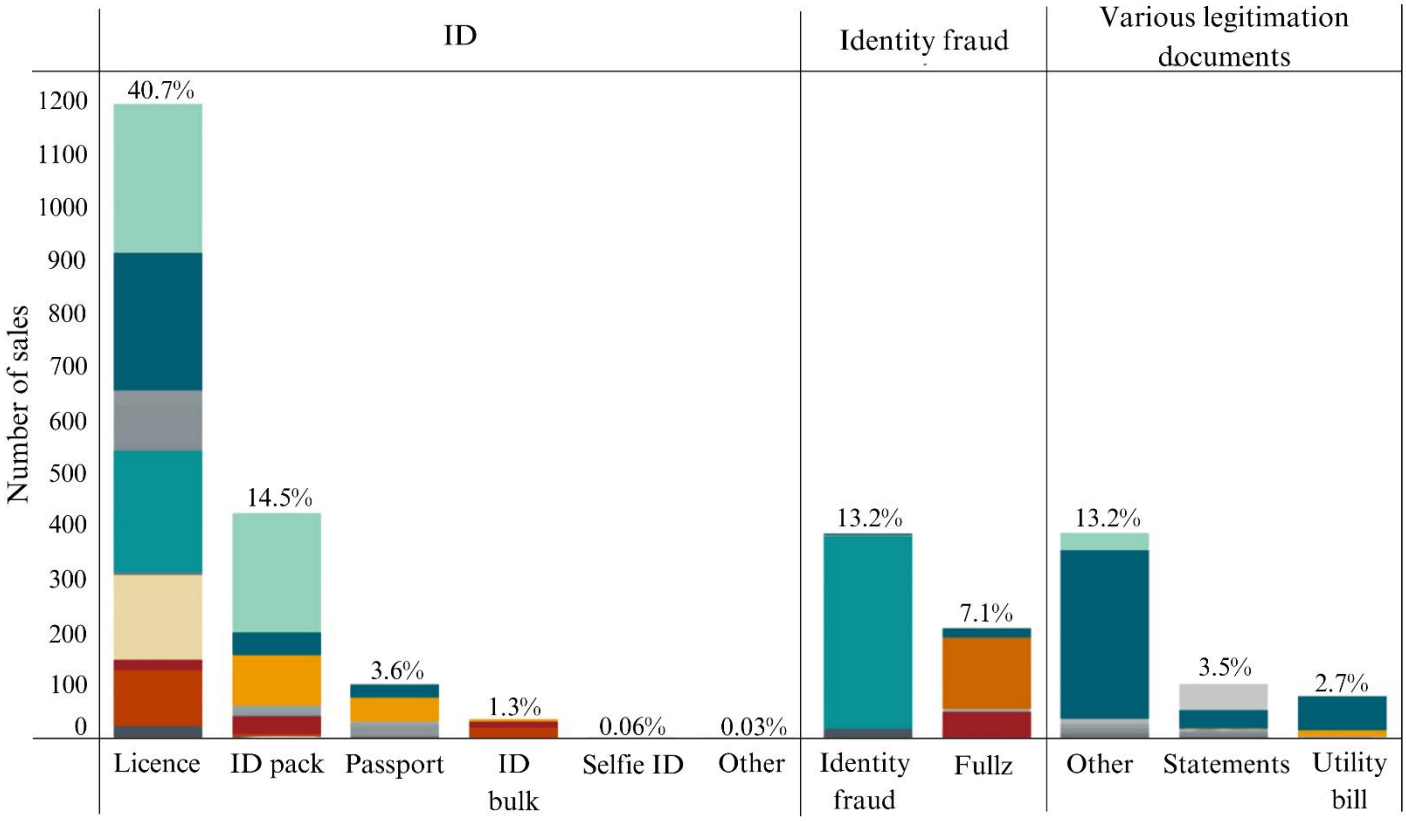


Figure 3-16: The number of sales per document type (Australian documents) on Empire. Both physical and digital documents are included here, and each unique colour is indicating a different vendor username

As outlined below in Figure 3-17, while these three vendors have sold products across other categories, largely illicit drugs and fraud-related (in line with previous research that showed Australian vendors typically diversify their activities across market categories [117]) they have specialised within the ID-related market, in that they only offer Australian documents. Furthermore, all three of these most prominent vendors within the Australian document market indicate that they ship their products from Australia. This prolific offender analysis may point to relevant targets for law enforcement to indicate potential top contributors to the market, further illustrating the potentially domestic nature of the Australian ID-related market.

All sales from the top vendors were for digital documents, except for one (known as Vendor #1 in this work), who had 69 sales for one counterfeit driver licence listing. Upon further analysis it was found that Vendor #1, is not just a significant contributor to the Australian ID-related market, they are self-claimed to be one of Australia's top vendors, with products spanning all categories, including the illicit drug category as illustrated in Figure 3-17.

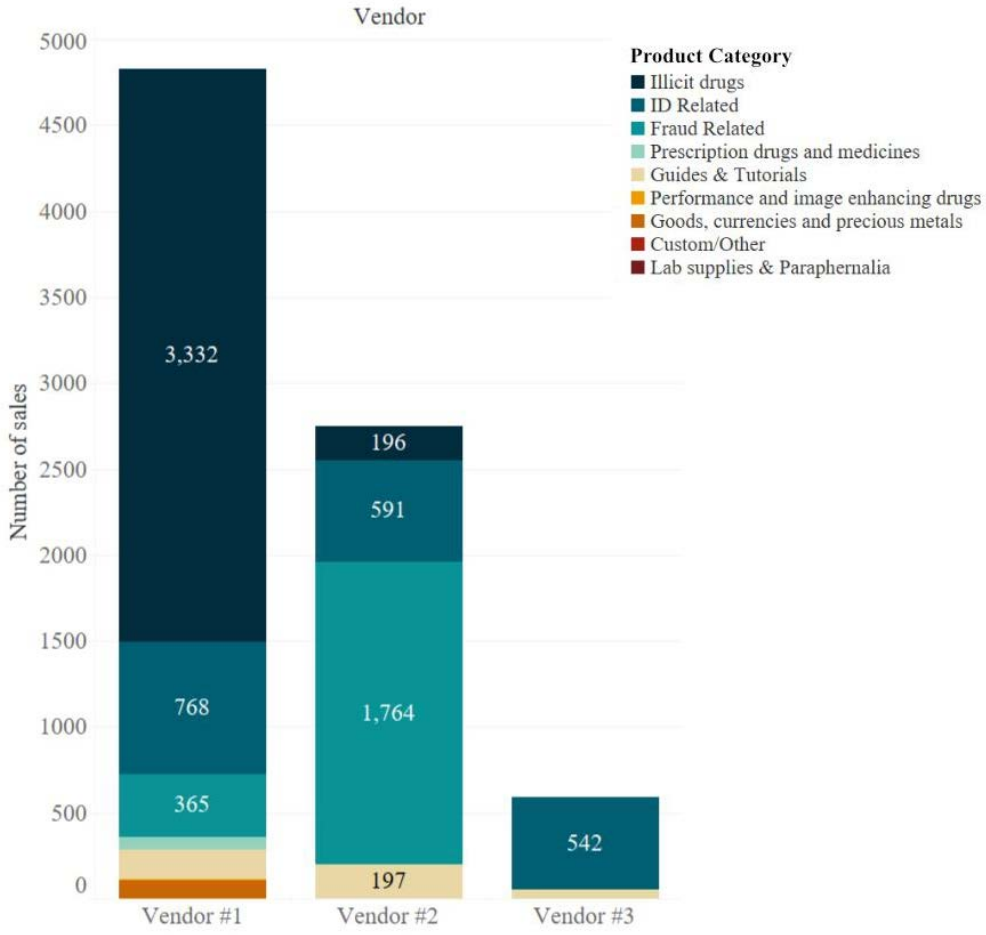


Figure 3-17: Number of sales per category across the overall market on Empire for the top three Australian ID-related vendors

Across the overall market on Empire, they have 4,825 sales and a total sales value of over $1.6million, placing them in the top 30 vendors (out of the 2,806 vendors on Empire) regarding total value of sales. This vendor, according to their vendor profile, previously operated on ten

different cryptomarkets in addition to Empire Market and WHM, perfectly illustrating the breadth and resilience of their operations. If this vendor was identified and removed from the criminal environment, the number of sales and supply to the dark web may be reduced, not just in the ID-related market, but also in the illicit drug and fraud related markets.

The three most sold ID-related products from Vendor #1 are (in decreasing order), a 'high quality' scan of an Australian driver licence (no state specified), an 'Australian person loan application package' including proof of identity documents, and a physical counterfeit Victorian driver licence. While the scan of the driver licence is not a surprising product to come across, the loan application and Victorian physical licence may provide some insight into the criminal environment.

By looking at the types of products that are popular within the illicit market, it becomes possible to detect trends between the products being sold on the digital market and crime trends occurring in the physical world. During COVID-19 the Australian Bureau of Statistics identified that there was a rise in bank and credit-card fraud, particularly during the lockdown periods, with 11% of Australians experiencing personal fraud, a 2.5% increase since 2015 [303]. Given that Empire's operation spanned a portion of the COVID-19 pandemic (it was operational until late August 2020), this is a potential example of external societal factors influencing the supply and demand of products on the cryptomarkets. While, of course, this approach is not without limitations, from an intelligence perspective examining the behaviours, products and trends present in the digital marketplace can provide insight into trends in the criminal environment beyond the digital world. It was interesting to note that most of the physical counterfeit licences for sale (including the 69 from Vendor #1) were Victorian licences. These documents have fewer security features compared to other states licences such

as NSW or QLD licences. Objectively, from a manufacturer perspective, the Victorian licences may be an easier target for counterfeiting, or it could be indicating a degree of familiarity between the vendors and a particular state's licence. From an intelligence perspective this could help to indicate to decision makers that the Victorian licences require an increase in security features to make it harder to effectively counterfeit them.

3.5 General discussion and conclusions

In comparison to the overall market the ID-related market is quite small with listings and sales for this category of products making up less than 4% of the listings on both markets (1.9% of WHM and 3.4% on Empire) and 2.4% of the sales (on Empire). The ID-related market was largely dominated by listings and sales for digital products (95% of sales on Empire and approximately 80% of listings across both markets). One category that is composed entirely of digital products is the identity fraud related category, which attracts a significant amount of attention within the cryptomarket-facilitated ID-related market, with 60% of the ID-related sales on Empire being for products that fall within this category. Across the entirety of the ID-related market on Empire, fullz were the product with the highest number of sales (42% of the sales) and the highest sales revenue at $435,345 (24% of the ID-related market revenue). The popularity of this product type is not surprising given that, according to the AIC, personal information such as name, date of birth and address (among others) are some of the most targeted, and misused pieces of information within identity-related crime [30], all of which are found within a set of fullz.

Identity fraud related product listings that featured products from the U.S. had the highest number of sales (87% of the identity fraud related category), mirroring the high levels of identity crime within the U.S., specifically identity theft and personal data breaches [288, 289]. Previous studies that have focussed on the online fraudulent document market have neglected to consider the identity fraud related portion of the market, with the sale of personal information and the like not being considered or being sorted into the fraud related category. It is important that these products be considered as part of the ID-related market, rather than focussing solely on fraudulent documents, as those items within the identity fraud related category can be used

for proof of identity in the online world and are an integral part of the identity crime related criminal environment. As illustrated by the popularity of U.S. identity fraud related products (52% of ID-related sales, and 87% of the sales within the identity fraud related category), and the increased rates of identity-related crimes and personal data breaches between 2018 and 2021 [288, 289], examining the sales and listings of these products can also provide insight into this digital criminal ecosystem. It is crucial to remember that the identity crime and fraudulent document criminal environments are intrinsically linked, with criminal activities that fall under identity crime often contributing to or enabling crimes that are occurring within the fraudulent document criminal environment, or vice versa.

The ID-related market on WHM and Empire was found to have a small number of vendors supplying a larger portion of the market, consistent with a previous study of the cryptomarket Agora [202]. This suggests there may be prolific offenders operating within the cryptomarket-facilitated ID-related market, much like what has been noted within the physical document market [15, 141, 142]. However, it appears that this structure is not unique to the ID-related portion of the cryptomarket, as there are prolific offenders also operating within the overall markets on both WHM and Empire. Interestingly, despite this presence of prolific offenders, the HHI calculation indicated that the ID-related market on Empire was quite competitive, with the vendors sharing a roughly equal portion of the market. This makes sense, given that 199 of the 234 vendors contributing to the ID-related market on Empire had a market share of less than one or zero as they were contributing very few sales to the overall marketplace.

It has been suggested previously that police and law enforcement actions have little impact on the overall criminal environment [247], however, recent research has illustrated that police actions against marketplaces helps to not only prevent markets from growing unchecked, but

also impacts the overall criminal environment, destabilising it in the wake of a large market closure [229]. This research, in combination with previous studies illustrates that a dual approach should be implemented by police, utilising research and forensic intelligence to inform their strategies, and to assist in the identification and neutralisation of prolific offenders that are significantly contributing to and profiting from the market as well as identifying and shutting down large markets as they emerge. Given the prolific behaviour that has been identified within this analysis, not just within the ID-related market, but also the overall market, the neutralisation of an individual vendor, such as Vendor #1 discussed in Section 3.3.5, could potentially reduce the supply of fraudulent Australian documents to the online market, as well as numerous other products such as illicit drugs. Of course, identifying those offenders that are most significantly contributing to the criminal environment should be based on a combined analysis of those that have the highest sales, listings and sales revenues. This can also be combined with a cross-market analysis of usernames and PGP keys to identify those vendors that are operating across multiple platforms, and organisations that are controlling multiple usernames. By using these online markets as vessels of information and intelligence to assist in understanding the marketplace better, but also to identify those most prolific vendors, the impact on the criminal environment may be increased, rather than the more reactive closure of markets. These analyses also enable the examination of often difficult to access illicit markets, providing quality intelligence that can increase the understanding of the criminal environment and therefore facilitate more targeted, and impactful action.

Examining trends in the trafficking and distribution of the physical fraudulent documents enables a better understanding of where the supply of these documents could be originating, providing some insight into potential avenues through which police and law enforcement might

be able to intercept shipments and deliveries of these illicit products, as has been done for the illicit drug market [96].

From the analysis of the trafficking patterns of the ID-related market it was identified that the U.S. and Australia seemed to have largely domestic markets for physical fraudulent documents. Interestingly, a correlation was identified between the origin country and the types of documents being offered by vendors, with most of the sales of U.S., U.K. and Australian documents being shipped by vendors originating from within the respective country. This is not surprising, as the ability to manufacture a quality counterfeit or forged document is undoubtedly linked to the manufacturers access to genuine documents of that kind. Even external to considering language barriers and how that might impact document quality (which has been suggested in previous research [17]), familiarity with the document that is being replicated would likely impact the perceived quality of the item by online buyers. It is therefore unsurprising that this correlation between origin and shipping country was identified, and that all three of the top vendors of Australian documents on Empire indicated their origin country as Australia.

Of course, while Australian documents are the second most listed and sold documents within the ID-related market, when focussing solely on the physical documents these conclusions are being based on what is, objectively, a small number of listings and sales. So, while this information can provide suggestions or indications of potential trends in the shipping and distribution of these items, the size of this data set needs to be kept in mind. If the research was expanded to include more markets, a better idea of this trafficking of the products could be gathered, especially when considering that there is the potential to be some variation based on the location of the market and what portion of the global population it is largely catering to.

Furthermore, the analysis of the manufacturing and trafficking of a market that is dominated by digital products will be intrinsically limited, as only a fraction of the market will ever be examinable. This is furthered when considering that the creation and transfer of these digital documents may just be an initial step prior to their manufacture into physical documents. Undoubtedly, a large portion of digital documents are used for proof of identity in the online world, but given the presence of 'document precursors' (i.e. components used to make identity documents such as holograms, barcodes, and security overlays) on these cryptomarkets, and the recent increases in their trafficking [51], it is entirely possible that some of these digital documents are being used to assist in the manufacture of physical documents, introducing a secondary distribution and manufacture location. The potential use of these digital items (personal information, fullz etc.) and digital documents (scans, templates etc.) to create physical documents is often not considered, especially in relation to those products within the identity fraud related category. More rigorous and consistent rules and regulations are required regarding the illicit manufacture of these documents, and the trafficking and manufacture of the different precursor components, both the digital and physical items. This is of particular importance when considering the recent implementation of AI to assist in the creation of personalised digital identity documents that have been successfully used to fool digital identity verification systems in cryptocurrency exchanges [241].

The importance of consistency in regulations and rules regarding document fraud and identity crime becomes even clearer when considering the extent and breadth of the online fraudulent document market. Cryptomarkets are not the sole avenue through which to purchase fraudulent identity documents and personal information online, with previous research illustrating that the online fraudulent document market spans across all levels of the web and includes dark web vendors that operate outside of the jurisdiction of cryptomarkets, operating independent shop

fronts [199, 200]. Not only are the size and costs associated with the ID-related market likely far greater than what is estimated in this research but given the results of previous research that has examined these other avenues of the online market, it appears that the supply and demand of products may vary based on the location of the shop front within the digital space.

Holt and Lee (2020) conducted a crime script analysis of fraudulent document vendors across the open and dark web, including single vendor store fronts on the dark web [200]. From their examination of these vendors profiles, they identified that most vendors sold passports (40%), followed by identity cards (25.2%), and driver licences (19.6%) [200]. They also found that the most common listed documents were for those from European (EU) member states (51.2%), followed by Asian (11.7%), South American (8.4%) and SWANA (7.2%) nations, with Australian/New Zealand documents only accounting for 3.6% of the products listed [200]. These findings contrast against those identified in this examination of Empire and WHM, along with other previous cryptomarket analyses, that have more or less agreed that the most prevalent document types on these markets were driver licences, particularly from more western countries such as the United States and Australia [47, 51, 202].

While the study conducted here and those mentioned above focussed almost exclusively on the dark web and cryptomarkets, Holt and Lee's study examined 19 vendors that spanned all levels of the web, with eleven vendors operating open web shop fronts, eight dark web vendors operating dark web shop fronts (external to cryptomarkets), and only three vendors operating within the jurisdiction of a cryptomarket [200]. The disparity between the sample type examined by Holt and Lee and the contrast between their results and those obtained from solely cryptomarket focussed analyses suggests that there may be a correlation between the popularity of document types, and document countries, based on the dominant geographic locations of the

users. As an example, WHM, Empire and Agora (which was examined by Baravalle et al. 2016 [202]) were all English language dominant markets, which are predominantly populated by users from the U.S, Australia, and the U.K [104, 110, 117, 249], reflecting the most popular document countries. Further, all three of these countries allow the use of a driver licence as a form of proof of identity, perhaps suggesting another correlation between document type and user locations, as driver licences were the most popular document type on WHM and Empire. EU member states on the other hand (as examined in Holt and Lee) do not allow the use of a drivers licence as a proof of identity, relying more on identity cards and passports, which seems to be reflected in Holt and Lee's results [200]. So, it is clear that the area of the market being studied, the dominant language of it in combination with the geographical and geopolitical climate of the participating countries likely impact the types of products being sold, resulting in some biases when conducting these analyses on singular marketplaces or regions of the online market.

Overall, it is clear that not only does the fraudulent document and personal information market span all levels of the web [199, 200], but there seems to be a variation in the product types that are the most listed and sold based on the location of the market within the online space, and what buyers that market is catering for. While only two markets have been studied here, one of which closed shortly after the crawling began, it is clearly impossible for any one study focussing on a single portion of the market to properly illustrate the breadth of the ID-related market, particularly when considering costs and damages associated with the sale and distribution of these products. A multi-source approach to this online criminal environment is required, coupling analyses of multiple cryptomarkets, with analyses of open web and independent dark web store fronts including alternate avenues of access such as forums and messaging application such as Telegram [304]. This in combination with examination of

statistical research conducted on the identity crime criminal environment, such as that conducted by the AIC, and ACCC will enable researchers to put their best foot forward when trying to understand this complex criminal environment. After all, the information extracted from cryptomarkets, or any other online market, like any trace, is incomplete and therefore needs to be used in partnership with other sources of information [96, 104], both about the online market and the overall criminal environment to ensure the that most complete picture is created. Combining these avenues of research can help provide decision-makers with clear information about the document fraud environment, so they can make more informed decisions about this criminal environment, and its key players.

Chapter

The Multi-source Approach for Document Fraud and Identity Crime

4 The multi-source approach for document fraud and identity crime

4.1 Introduction

The criminal environments of identity crime and document fraud are problematic, both on their own and in their facilitation of other serious and organised crime [16, 32, 37, 47, 51, 92, 135-139, 305]. However, very little is known about these criminal spaces, with inconsistencies in definitions and laws coupled with reactive law enforcement resulting in an ill-defined criminal environment that is consistently increasing [29, 30, 44, 46]. The previous chapters of this work (Chapter 2 and Chapter 3) introduced two approaches, being the profiling of fraudulent documents and cryptomarket analyses that can be used separately to proactively tackle this criminal environment and provide more information about identity crime, document fraud, and the crimes that they may be used to enable.

It is clear, both from previous research and that conducted here, that document fraud and identity crime do not exist solely within either the digital or physical space, and that 'fake IDs', to use the colloquial term, are not being used wholly by underage individuals to access alcohol and other restricted services [51]. Rather, that the criminal environment is expansive and spreads across all levels of the web, as well as throughout the physical space, with fraudulent documents and personal information facilitating a broad range of crimes, from simple misdemeanours through to transnational, serious, and organised crime (TSOC) [32, 51, 140].

While the profiling of fraudulent documents and cryptomarket analyses are effective at providing insight into criminal environments [96, 104, 117, 203, 247, 257, 260, 261, 267] and internationally have assisted in the identification and proactive dismantling of organised crime rings [11-13, 15, 16, 37], when used in isolation they provide a very one-sided view of the

market, contributing to information siloes and linkage blindness [153]. A more holistic view, in line with the ethos of forensic intelligence and intelligence-led policing can be gained from combining these two seemingly dichotomous areas of the criminal environment.

This chapter will explore how these different methods of analyses can be used together to provide a much more comprehensive understanding of the market for personal information and document fraud. It will illustrate how combining the results of trace analyses (such as those from physical documents and digital information sources e.g. cryptomarket examinations) with alternative sources can inform intelligence-led policing and decision makers in how best to proactively address identity crime, document fraud, and organised crime and how this could fit into a holistic approach to increase the understanding of the overall identity crime and document fraud criminal environments [96, 104].

4.2 Aims and objectives

In this chapter, the two often separate sides of the illicit marketplace are examined, and the importance of using them as part of a multi-source approach towards understanding the criminal environment of identity crime and document fraud is discussed. Further, the potential of using these two information sources as part of a broad, holistic multi-source approach, combining information from a range of sources including police seizures and government reports as part of an integrated information sharing network is illustrated.

The following objectives are addressed:

1. The evaluation of both data sources, being the visual profiling of physical documents and the cryptomarket analysis to suggest how these tools can be incorporated as part of a holistic multi-source approach for understanding identity crime.
2. The examination of trends in the identity crime environment within Australia and how these relate to the examination of both the physical and digital markets.
3. To outline how a multi-source approach encompassing a broad range of information sources, including the examination of both physical and digital markets can assist intelligence-led policing and provide a better, more holistic understanding of the criminal environments of identity crime and document fraud within Australia.

4.3 The online and physical criminal environments, two sides of the same coin

Despite the obvious differences between the online and physical portions of the market, the results in Chapters 2 and 3 of this thesis illustrate that the structure and behaviours of vendors within the physical market are reflected by those individuals that are operating within the digital market, and vice versa. These results suggest that both sides of the market exhibit a similar degree of organisation, with prolific offenders providing a disproportionate number of the products for the market. Out of the documents examined in Chapter 2 (n=183) 94% of them were linked to at least one other document, with the two largest series, VIC_DL1 and NSW_DL1 covering 30% and 17% of the document set, respectively, indicating that there may be prolific manufacturers contributing to the Australian document market. This potential organisation was also noted within the online market on Empire and WHM, with 65% of the sales for Australian documents originating from only three vendors.

While, in both cases, the data examined was only a small snapshot of the overall illicit market for Australian documents, it does provide a valuable first look into its structure and organisation. It should be noted that this level of organisation, and the presence of these prolific offenders wasn't unique to the Australian fraudulent document market, and was noted across the broader ID-related market, mirroring the structure that has been noted internationally within the physical market [13, 15-17, 143]. This correlation between the physical and digital market across the international canvas of identity document fraud suggests that this structure and organisation is typical of the document fraud criminal environment and therefore is likely to also be present within the broader criminal environment for identity crime. Overall, this suggests that the Australian fraudulent document market may be a repetitive and pervasive

crime problem punctuated by prolific offenders much like what has been identified internationally.

Outside of providing insight into the market structure, these two data sources can also suggest document templates and security features that are particularly vulnerable to counterfeiting and alteration. Within WHM and Empire some of the most listed physical counterfeit Australian documents were the VIC licences, which while more secure than the WA licences (as outlined in Chapter 2 Section 2.3.2.4), had fewer security features and template features than the NSW licences, perhaps making them an easier target for fraud, or indicating a larger number of forgers based in Victoria (i.e. as they have greater access and familiarity to these documents). The work in Chapter 2 also outlined that the most vulnerable security feature across all the counterfeit licences examined, were the OVDs with over 70% of each licence group successfully replicating these features. Interestingly, within WHM there were 48 listings for ID document components and security features. 40 of the 48 listings were for OVD overlay stickers marketed to be used in counterfeit licences. While these weren't for Australian licences, their presence within the market, in combination with the high percentage of documents in Chapter 2 that had accurately replicated OVDs, suggests that these features cannot be relied on in the authentication step for counterfeit documents, or that at the very least, these features need to be examined more closely. However, as illustrated in Chapter 2 Section 2.3.2.3 the OVD layer is uniquely useful in preventing the alteration or forgery of Australian credit card style documents, or at least making it easier to detect, particularly those that are designed to be irreparably damaged by any form of tampering or removal.

One of the core principles discussed within the National Strategy for Identity Resilience (2023) is the need for Australian governments to have consistent standards and approaches towards

identity resilience [306]. This can be accomplished by ensuring that all jurisdictions are working towards common objectives, standards, and practices, and through greater consistency in identity document security [306]. There is no doubt that this is a legitimate need within Australia, especially in relation to the standardisation of document security and this can, in part, be achieved by examining both the physical and online portions of the market. Before national document security standards can be introduced, research into the current methods of counterfeiting and circumventing security features needs to be done. The combination of these two data-sources, especially if the scale of the visual document profiling was increased to include documents collected across a broader time frame and across multiple jurisdictions, can assist the Australian government in reaching these standardisation goals. Furthermore, as illustrated above, this method can provide crucial intelligence to document manufacturers and frontline document authenticators as to what features should be updated and targeted during the authentication process.

Of course, while the markets do seem to reflect each other in structure, the presence of prolific offenders, and in some of the product types and trends, there are some valuable differences in that each side of the market captures different information. In the physical side of the market, most of the documents examined in Chapter 2 were counterfeit licences, with a smaller number of forged photo cards and four pseudo documents. While the cryptomarkets also had an overwhelming number of counterfeit licences being listed and sold, there were far fewer forged documents, and no pseudo documents at all. However, there was a second category of products that were very popular across both Empire and WHM that were not seen in the physical market, or at least not in the same form.

The market for stolen and fraudulent personal information, including products such as fullz and identity fraud packs (as outlined in Chapter 3 Section 3.3.2.1), is a significant part of the identity crime and document fraud criminal environment that can easily be overlooked if the physical side of the market is examined in isolation. The prevalence of these exclusively digital items within the cryptomarket facilitated online ID-related market indicates that these are a considerable problem within the identity crime criminal environment, especially with increasing data breaches and identity crime rates [29, 30, 44, 45, 288, 289]. Furthermore, these digital products have the potential to cause significant harm to the individual whose information has been compromised, with vendors able to resell these products multiple times, with ease. Digital products can also be distributed with a lower risk of detection for the vendor, as using the internet as a distribution method is far more reliable and safer, removing the potential for their products to be detected and intercepted through traditional postage routes, particularly when crossing borders [307]

While it is natural to assume that the portions of the market that exist within the digital and physical space would be separate, these two different sides of the market are intrinsically linked. Of course, document manufacturers use the online world to distribute their physical documents. However, what is less obvious is that document precursors, such as security features and substrates are also being purchased from online vendors[26], likely to be used in the manufacture of physical documents as illustrated in Figure 4-1. There is of course the fact that these are not the only precursors being sold, with the scans, templates, and identity fraud products that dominate the cryptomarket also potentially being used to facilitate the manufacture of physical documents [51].

[26] On Empire and WHM

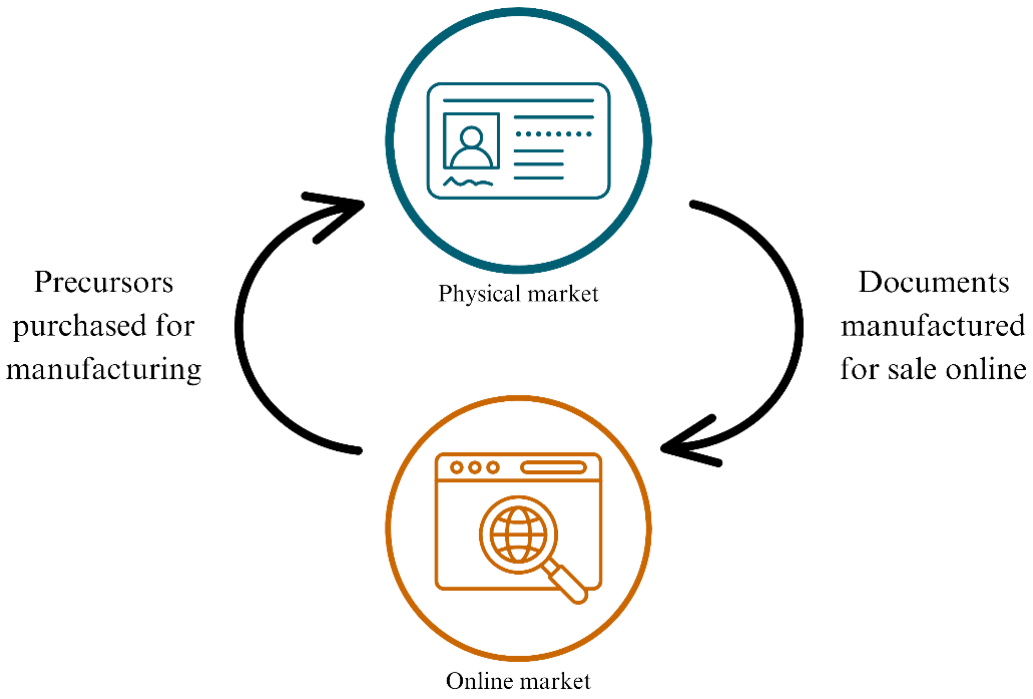


Figure 4-1: Relationship between the online fraudulent document market, and the physical documents intercepted during profiling

While the information provided by the examination of both the cryptomarket facilitated market and the physical market for fraudulent documents is highly valuable, this combined analysis is still not sufficient to provide a holistic understanding of the illicit marketplace. As mentioned previously, the online portion of the market[27] spans all levels of the web [199, 200, 269], and there are products that exist within the open web that were not present within either WHM or Empire Market. Within Chapter 2, four pseudo documents were collected from local NSWPF stations, and after they were visually profiled, two series emerged (Chapter 2, Section 2.3.2.1). A search was conducted through Google to investigate the potential sources of these pseudo documents, and to see if there were any links to those that were available through the open

[27] Please note that when referring to the 'market' generally this is referring to all levels of the online or physical marketplace, and not just one level such as the cryptomarkets.

web. Similarities between the seized documents and those offered by a well-known ‘novelty’ fake ID vendor were identified. Previously, this vendor had been the subject of an investigation, as reported by the Sydney Morning Herald (SMH) in 2013 [308], and this article contained two examples of documents from that vendor. Aside from sharing overt visual similarities, both documents included in the SMH article had the same document number as those collected from the NSWPF, indicating this website was likely the source of these documents. Examples of the product images used by this website are included below in Figure 4.2, with the corresponding documents intercepted by the NSWPF provided below them.

Figure 4-2: Documents (a) and (b) from the well-known 'novelty document' manufacturer in the open web [305], and documents (c) and (d) that were intercepted by the NSWPF

Vendors such as the one mentioned above, skirt the laws regarding the manufacture of fraudulent documents by marketing them as ‘novelty’ items with disclaimers indicating that

their products are ‘not to be used as real identification’. They are also careful to ensure that while the document may appear visually similar, they are not claiming that they are legitimate documents. As an example, the ‘Student Identification Card’ has overt visual similarities to a full NSW driver licence (Figure 4.2). It appears that by existing within small loopholes of the law, and by putting the legal onus on the purchaser of the documents, this vendor, and others like them, can exist in the realm of the open web, escaping scrutiny. However, open web store fronts aren’t solely providing pseudo documents, with a range of websites offering counterfeit, and even ‘100% legit’ documents for sale.

It is also becoming even more impossible to consider the physical and online sides of the market as being entirely separate due to the increase in digital technologies embedded within the identity document space. With the introduction of documents such as the NSW digital driver licence (DDL) and increases in the use of digital documents for online identity verification (e.g. for rental applications, PayPal etc.), more products and items are beginning to exist at the cross-roads between document examination and digital forensic science, so only focussing on physical traces within the document fraud space will result in a significant portion of the criminal environment being overlooked.

This becomes especially relevant when considering the recent use of Artificial Intelligence to generate personalised images of counterfeit identity documents that have successfully been used to fool Know Your Customer (KYC) identity checks for services such as cryptocurrency exchanges [241, 309-311]. The implications of the use of AI in the generation of digital identity documents is serious, with the website examined by 404 Media, OnlyFake, claiming to be able to mass-generate these documents, creating upwards of 20,000 documents in one day [241]. Given the fact that these AI generated images contain attempts at replicating the visual and

security features present on the identity documents, there is the potential that the visual profiling method could be used to help group those documents that are originating from the same source. However, for the visual profiling method to work the images that the AI produces would need to have some replicated visual elements or show some degree of similarity between different images so that they could be visually profiled and linked back together. Of course, this is entirely reliant on how the AI works, along with how it has been trained and what images have been fed into it, as the quality of the images that it has been provided with, coupled with the extent of its learning will dictate how accurate the visual elements of the document will be. By solely generating digital documents, it circumvents some of the security elements that have been designed to prevent accurate replication, reducing the number of features that could be included in a profile (e.g. microprinting). This new form of identity verification document has created an opportunity to investigate the application of digital forensic science, and the profiling of digital traces (such as image metadata) to assist in linking documents produced by these digital sources.

Clearly, to properly tackle this criminal environment, a holistic approach is required, coupling analyses of the physical market with the entirety of the online market, especially when considering the evolution of digital technologies within the space of identity crime and document fraud. Figure 4-3 shows how these two areas of investigation can be partnered together as part of a systematic forensic intelligence framework, adapted from Morelato et al. in 2014 [1], and shown in Chapter 2 Figure 2-4. The beauty of this transversal framework is that it is easily modifiable, as illustrated here and in previous research [1, 91], and can be used for any trace analyses, thereby assisting in the reduction of the trace-specific and silo-reinforcing intelligence models that have been published over the last two decades [1].

Essentially, the information generated from the profiling of the fraudulent documents, and the online market examinations are combined at the analysis step, facilitating comparisons between both the physical and digital traces of the markets to create a more comprehensive understanding of the criminal environment, providing insight into the supply and demand of these items, their trafficking and distribution, the structure of the networks generating and using these documents as well as indicating what documents and security features are no longer effective at preventing counterfeiting.

Additionally, dumps of personal information are commonly listed and sold online, so the active crawling of forums and marketplaces (as examples) for this information this could help flag potential breaches prior to them being detected and reported by companies and individual victims, reducing the window of time the offender has to cause harm or gain benefits from using the victim's information. Of course, the value of these links and the intelligence that can be gathered from them would only increase if more contextual information about the seized documents had been collected and shared, enabling the analysis of trends over time and the identification of emerging modus operandi. This would enable the intelligence generated from these analyses to impact not only the tactical intelligence level, but also the operational[28].

[28] Referring to the different levels of forensic intelligence explained in Section 1.4

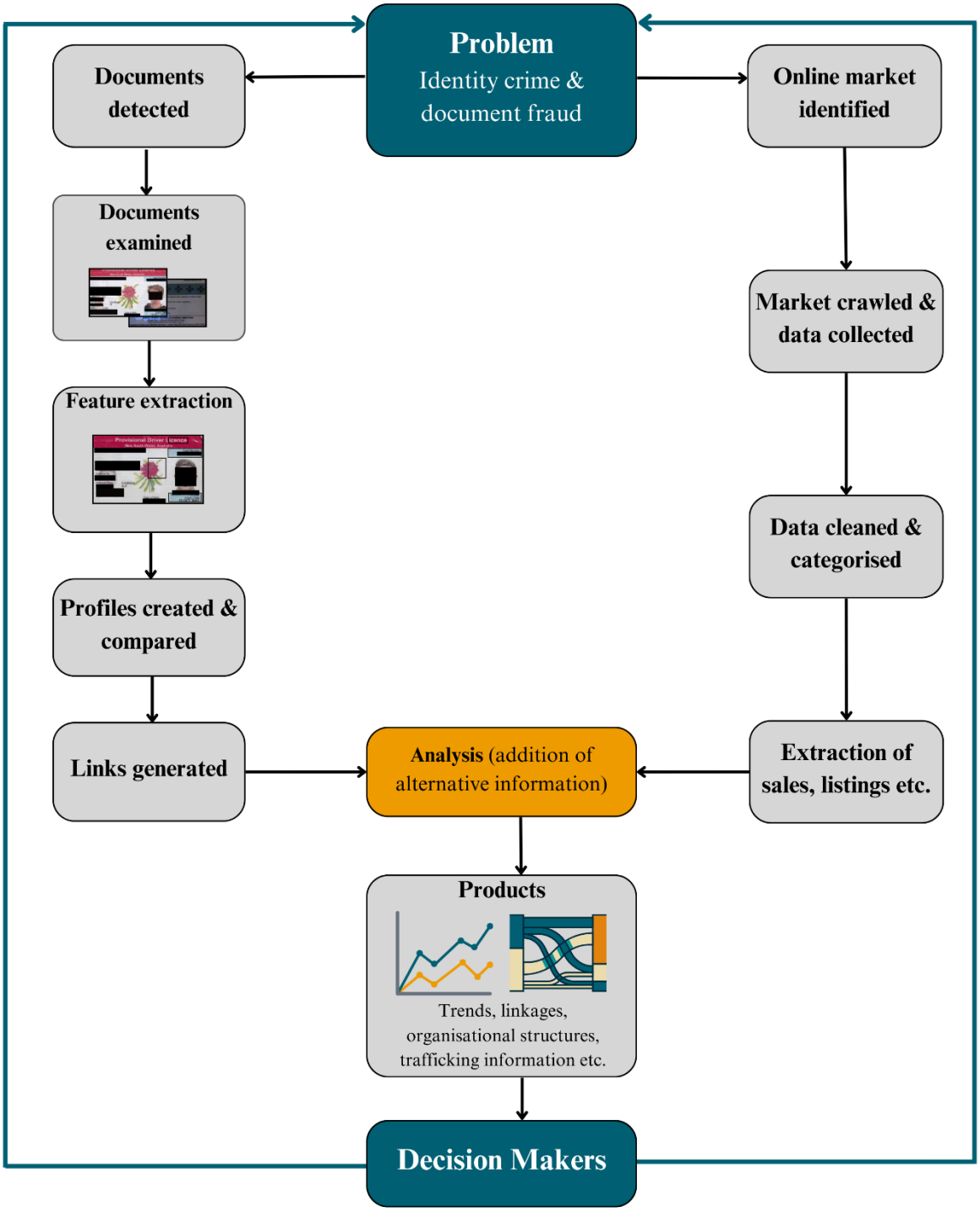


Figure 4-3: The systematic intelligence framework for the combined analysis of the market for fraudulent documents and personal information. Adapted from Morelato et al. 2014 [1] and modified to illustrate the combination of information from the profiling of fraudulent documents and the examination of the online markets. Please note the examination of online markets here is an example, any online means of document or information distribution could be included here.

However, the illicit marketplace is just one part of the overall criminal environment, which while important to understand, cannot provide a holistic understanding of the identity crime and document fraud criminal environments in isolation. To properly understand these criminal environments, a multi-source approach is required, not just including other areas of expertise within forensic science, such as digital forensic science, but considering a wide range of information sources, such as data from law enforcement and government organisations, criminological research, external stakeholders, and academia. Currently within this space there are numerous organisations that collect and/or provide information about identity crime, whether that be the reporting of offences to law enforcement bodies or reporting agencies, or research conducted through government organisations. Until all this information is combined and examined, the criminal environments of identity crime and document fraud will continue to flourish within the gaps made by inconsistent legislation, definitions, and policing priorities, which is the unavoidable by-product of the current siloed approach.

4.4 Arguments for the multi-source approach

One of the main barriers to reaching a holistic understanding of the identity crime and document fraud criminal environment in Australia is the sheer number of organisations that work within the identity crime space, and the division between them. In relation to identity crime and theft there are several reporting agencies (not including police and law enforcement) and organisations that provide information and guidance to victims of identity crime. Across the identity crime information pages of the AFP, Victorian Police, NSWPF and Office of the Australian Information Commissioner (OAIC) they each recommend different reporting agencies and information bodies including IDCare[29], ScamWatch[30], ReportCyber[31] and ID Support NSW[32] [312-315]. However, simply reporting this incident to one agency is not enough, with victims having to manually cancel their credentials and report the incident to upwards of 33 different organisations as illustrated in Figure 4-4 [44]. The burden of reporting and communicating this information falls squarely upon the victim, requiring them to not only do an extensive amount of work to ensure all relevant parties are notified, but also act as the conduit of information between these divided organisations [44].

[29] https://www.idcare.org/
[30] http://www.scamwatch.gov.au/
[31] https://www.cyber.gov.au/acsc/report
[32] https://www.nsw.gov.au/id-support-nsw

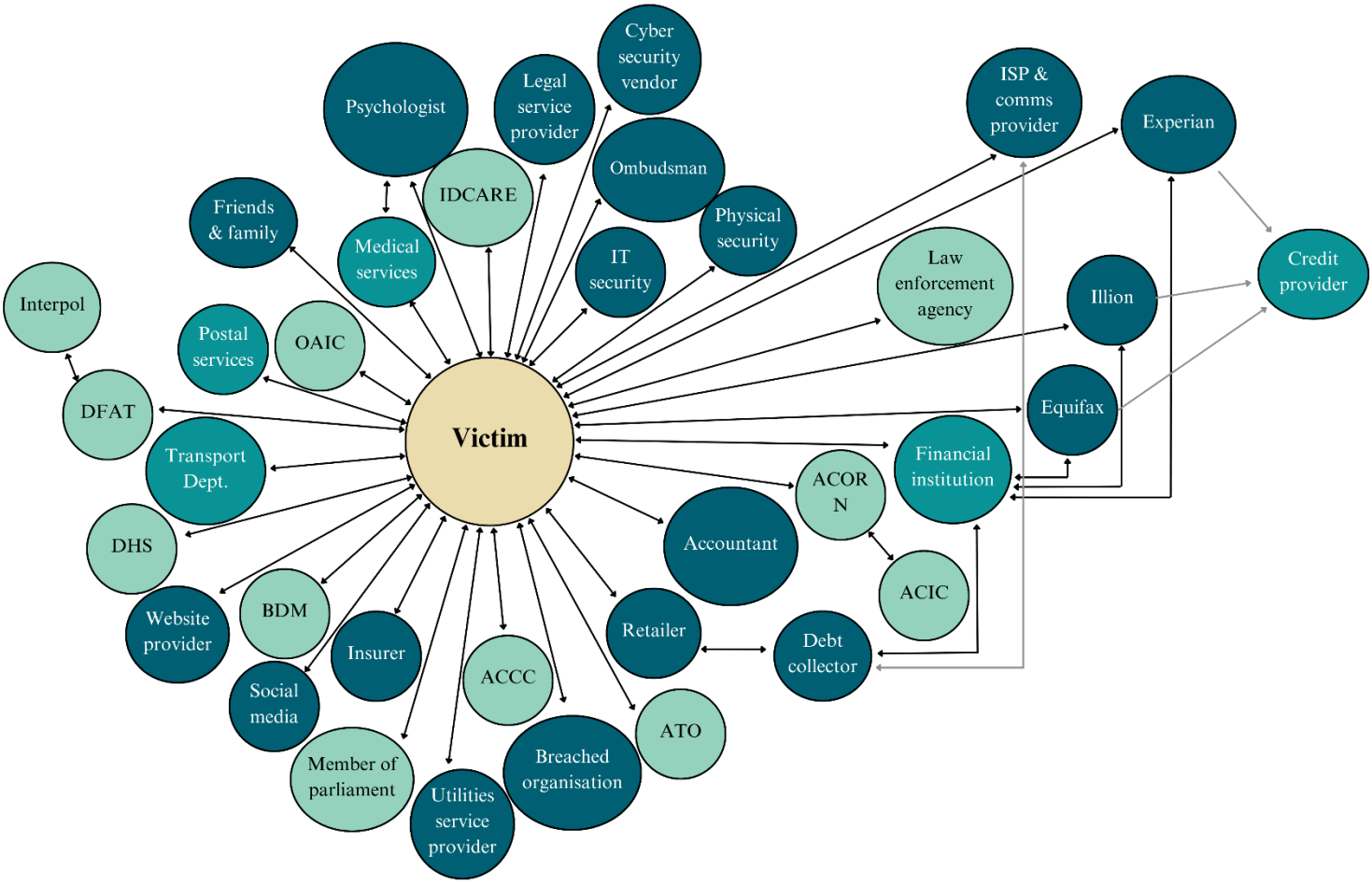


Figure 4-4: The social nodes in the identity theft response system, adapted from Wyre et al. 2020 [44], illustrating the extent of communication required from a victim of identity crime in Australia. ACCC = Australian Competition and Consumer Commission, ACIC = Australian Criminal Intelligence Commission, ACORN = Australian Cybercrime Online Reporting Network, ATO = Australian Taxation Office, ISP = internet service provider, OAIC = Office of the Australian Information Commissioner, DFAT = Department of Foreign Affairs and Trade, BDM = Births, Deaths and Marriages, DHS = Department of Human Services

Further muddying the waters are the numerous organisations that provide reports on or conduct research into the criminal environment of identity crime, including law enforcement-based organisations in addition to criminology and academic institutions [44]. Each of these organisations can provide information about a different part of the criminal environment, with law enforcement organisations obviously focussing more on crimes that are reported and

detected, and research bodies such as the Australian Institute of Criminology, providing insight into the victim's perspective and experience of identity crime through surveys.

While useful, due to the self-reporting and voluntary nature of surveys they are intrinsically biased, only providing the perspective of the victim [96]. Surveys will also typically target specific portions of the population, resulting in information gaps created by the sub-population being targeted and the specific questions that are being asked [96, 316], with many surveys focussing solely on personal identity fraud, neglecting that experienced by businesses [316]. Another significant gap is that victims rarely have full knowledge of the crime that was committed against them, with most not being aware of the method through which their information was compromised [44]. Information and reports based on law enforcement data are also intrinsically biased, as the focus of the agency will impact the crimes being detected and investigated. Therefore, the data produced may not be representative of the actual occurrence of identity crime and document fraud [96]. This is especially relevant when considering the severe under-reporting of identity crime and the information breakage across the different Australian reporting organisations and institutions [44].

Currently, everything that is known about the criminal environments of identity crime and document fraud is based on reactive reports, seizures, and research, focussing entirely on when the documents and personal information are being used to commit or enable a criminal offence. This focus on the end-use of these items is neglecting the mass of information that can be gathered by examining their supply chain, being their manufacture, sale and distribution (Figure 4-5). Not only can this provide extra information and insight into the criminal environment, but it also creates avenues through which these items and documents could be intercepted or detected, prior to their use to enable other criminal acts, thereby proactively

reducing the criminal environment of document fraud, but also preventing further criminal offences from occurring. An understanding of how fraudulent documents are being manufactured and distributed and how personal information is being accessed is crucial to properly understanding this criminal environment and thereby creating strategies to properly disrupt these criminal activities.

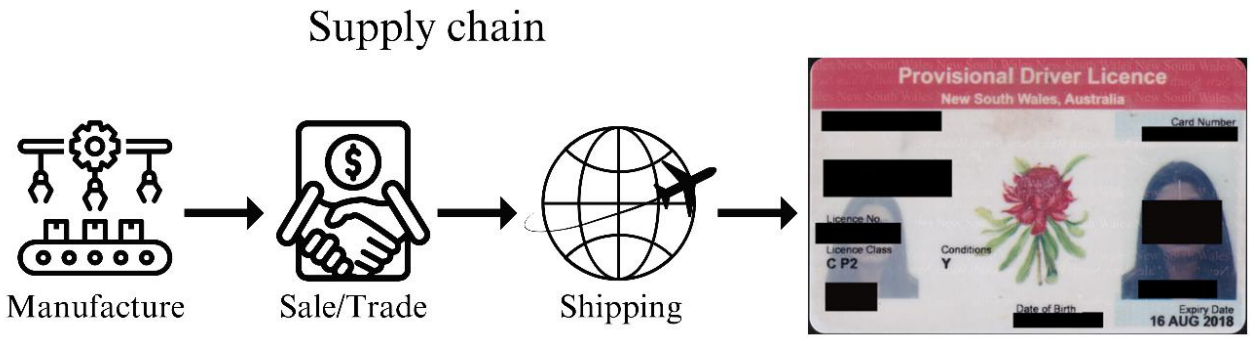


Figure 4-5: The illustration of the supply chain for fraudulent documents and personal information. Prior to their end-use fraudulent documents and personal information that are purchased/sold must first be manufactured or stolen/acquired and then will go through a sale/transfer process to reach the eventual user. This supply chain should be examined to extract intelligence that can further illuminate the overall market and criminal environment for identity crime and document fraud.

In essence, no single organisation, survey, or research body is properly encapsulating the identity crime criminal environment, with each avenue of information only providing partial insight. This results in each organisation only having a fragmented understanding of the criminal environment, which limits the impact that their decision making can have, especially given the communication barriers that exist between these organisations (as illustrated in Figure 4-6). The type of information required to properly characterise the distribution and trade of fraudulent documents and personal information is not collected, or at least not shared beyond the organisation in which the information originated, making it impossible to accurately estimate the overall problem of identity crime and document fraud.

Figure 4-6 illustrates the diversity in organisations that conduct work within the identity crime space. In all cases, not only is there a lack of information sharing between the different branches (i.e. research to law enforcement to the private sector) but there is also a lack of information sharing between organisations within a branch [44].

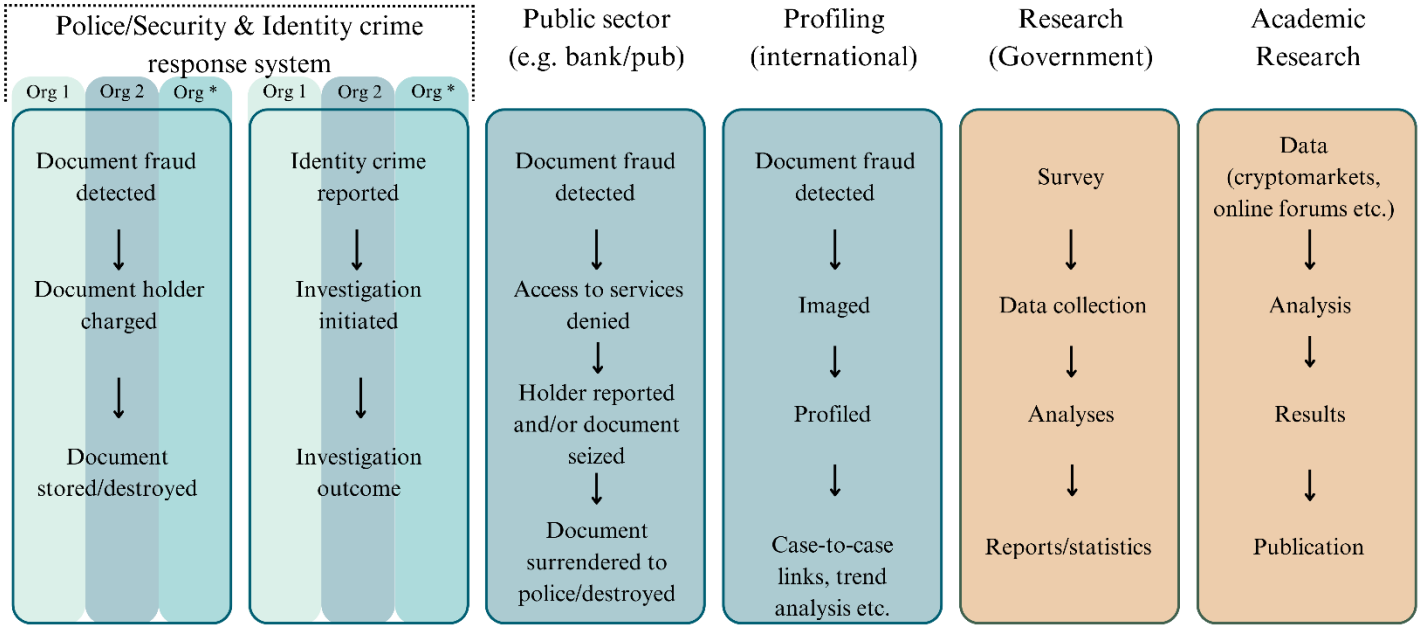


*Figure 4-6: Visualisation of the siloed approach to identity crime and document fraud information gathering and reporting. *There are numerous organisations involved in the ID Crime reporting system, these three are included as an illustration*

The only way to properly understand this criminal environment is to combine information sources, not just considering the physical and digital portions of the market but moving beyond that to consider the insight that can be provided by alternative information sources both within and beyond policing and security [97, 98]. The limiting factor here is of course the many barriers to information sharing that exist in general across government organisations, but particularly within those of law enforcement and security [198, 317]. If there is to be any chance of reducing, disrupting, and preventing identity crime and document fraud, and subsequently

the many other crimes they enable, then there needs to be greater information sharing between police and security organisations, along with other research bodies that are investigating the online market and the identity crime space in general. Not only would an integrated information sharing network streamline the identity response network, reducing the burden on victims, but it could help to properly understand and illustrate the breadth of this criminal market. Furthermore, with the integration of a document profiling system such as BIDIF, it could assist in the earlier, proactive identification of prolific offenders within the identity crime and document fraud criminal environments, along with those tangentially related criminal environments that are enabled using these illicit goods. Of course, before this can happen, the criminal environment for identity crime and document fraud must first be accurately measured, so that it can subsequently be properly managed [318].

4.4.1 The multi-source approach in practice

The concept of collaborating between research and policing organisations is not new, with some having been in place for over 100 years, as is the case for The School of Criminal Justice (*Ecole des Sciences Criminelles)* at the University of Lausanne in Switzerland, established in 1909 [319]. While in Switzerland the co-operation between police and academia has remained strong, as illustrated through the implementation of BIDIF and other collaborations [16, 97, 98], in most other regions there has been a gradual divide, resulting in the fields of academia, research, and law enforcement separating [320]. This is dangerous when considering that transnational, serious, and organised crimes (TSOC) cannot be properly disrupted, reduced, prevented, or even adequately policed without the use of consistent and broad collaborations and multi-perspective analyses [96, 198, 320-323].

In an attempt to improve these collaborations, the Australian National Strategy to Fight Transnational, Serious, and Organised Crime was proposed and agreed upon by The Council of Australian Governments in 2018. This strategy outlines the importance of transdisciplinary partnerships to properly tackle complex criminal environments through the implementation of a four-pillar approach to assist in national policy capability [324]. These four pillars focus on different levels of collaboration, education, and research to positively impact policing policy and strategies to better understand, and thus tackle TSOC. These steps are outlined below and have been summarised in Figure 4-7 [198, 324].

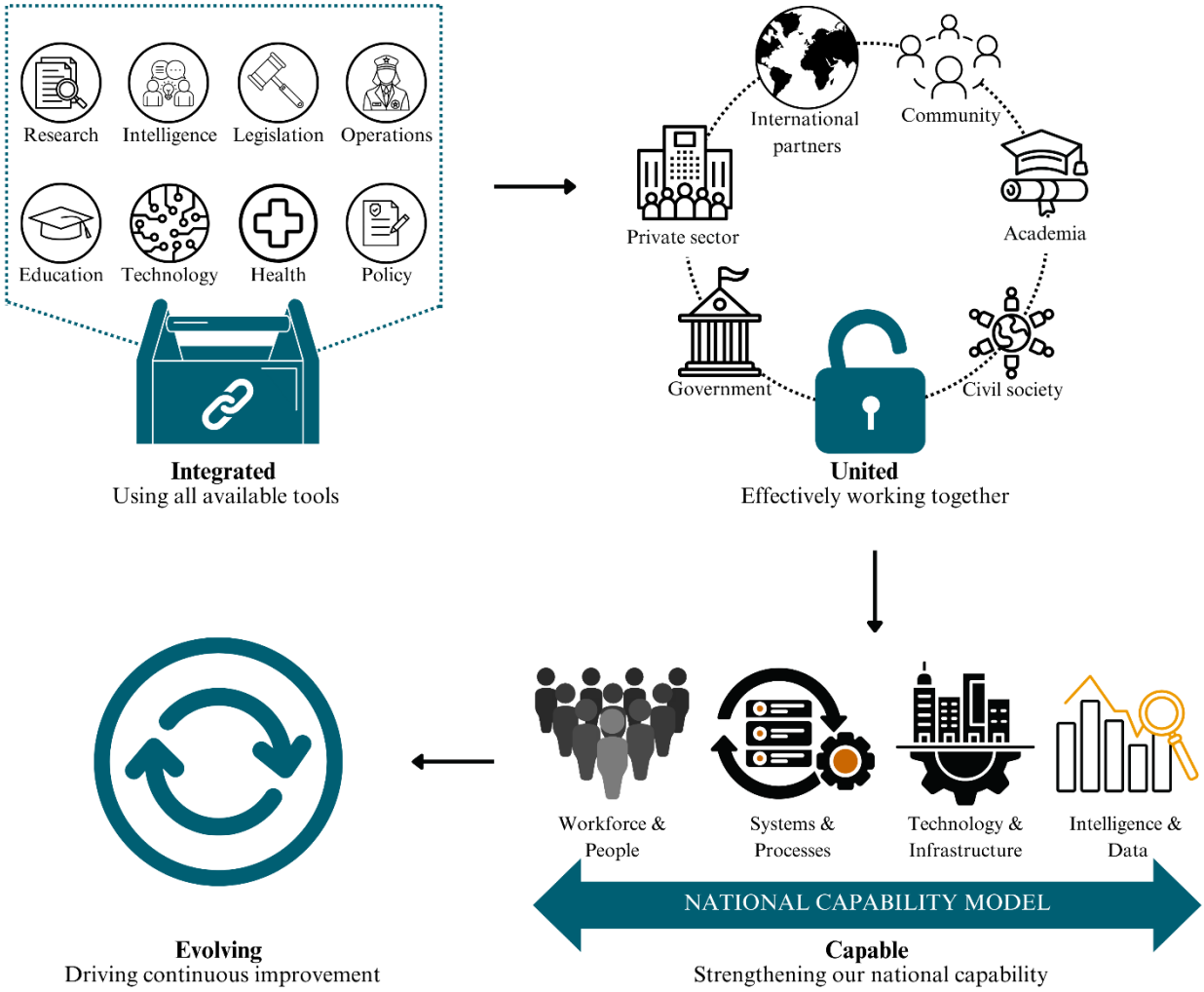


Figure 4-7: Summary of the four-pronged approach to transnational, serious and organised crime as outlined by the Commonwealth Transnational Serious Organised Crime Centre (CTSOCC). Adapted from [324].

The first pillar, *integrated*, focusses on enhancing the multi-faceted response to better disrupt TSOC criminal environments. The core of this pillar is its reliance on employing multiple tools from a variety of fields, including but not limited to research, education, legislation, policy, technologies and intelligence. These broad approaches should be implemented offshore, at the Australian borders, onshore and within the community to ensure organised crime is detected, disrupted, and prevented, ensuring the safety of Australia and its many communities.

The focus of the second pillar, *united,* underlines the importance of developing collaborative partnerships domestically and internationally across different governments, the private sector, the community, academia and civil society to work together effectively to achieve common goals.

To properly tackle TSOC criminal environments, a national capability model (the third pillar *capable)* was designed to better understand the roles of the four main national capabilities (being the workforce and people, systems and processes, technology and infrastructure and intelligence and data). This model enables the understanding of what capabilities are currently in use to disrupt this criminal environment, along with what gaps there may be and how they can be addressed in the future.

The final pillar, *evolving,* outlines the importance of feedback within the overall model. It is necessary to continuously improve approaches and the overall model through research, innovation, and ensuring that capabilities are accurately measured, outcomes are understood, and successes are recognised.

This illustrates that not only is cross-organisation collaboration possible, it emphasises that complex criminal environments are best handled when institutions co-operate and implement a broad range of tools, technologies and intelligence sources [324]. Identity crime and document fraud are criminal environments that clearly share features with other TSOC, in that they are organised, structured, and punctuated by prolific offenders [11, 15, 16, 51, 143, 172], with these criminal environments impacting individuals, communities, the private sector and the government [325]. Therefore, the main principles of the model explained above can be applied to the criminal environment of identity crime and document fraud.

The first step of this four-pronged approach to TSOC is reliant on expanding the tool kit of law enforcement and using all available tools to more proactively detect TSOC activities at Australian borders, onshore and within the community. An incredibly powerful, readily available tool, that is needed within Australia, as illustrated by the results of this research and the results achieved internationally, is the BIDIF system. The most logical first step towards better tackling the criminal environments of identity crime and document fraud, and by extension, TSOC, would be to implement BIDIF on a national level, focussing on profiling those documents that are encountered at the borders, on shore and within communities. This of course, requires some buy in, not only from law enforcement and government organisations, but also external stakeholders such as banks and licenced establishments, to ensure that all counterfeit and fraudulent documents, or at least the majority of them, are being examined and incorporated into BIDIF to provide the fullest picture of the Australian criminal environments.

As illustrated by the cross-organisational links identified in Chapter 2 Section 2.3.2.2, and in line with the second step in the TSOC approach [324] greater communication between organisations is required to properly tackle this criminal environment, and BIDIF can facilitate this communication while still protecting sensitive information, whether that be personal information on the documents, or case information from the organisations. As discussed in Chapter 2 Section 2.5, there are some steps that need to be taken within Australian organisations, largely revolving around the introduction of standardised practices for the collection and storage of fraudulent documents, as well as the creation of partnerships and agreements between Australian law enforcement organisations.

To ensure the smooth integration of this system, as well as information sharing between these organisations, discussions need to start being initiated between these organisations regarding

the implementation of this system, as this will undoubtedly take a significant amount of time. To properly understand this criminal environment there needs to be contributions not only from state and federal police, but also border control, intelligence organisations, as well as public sector organisations that deal with identity documents such as financial institutions, licenced venues, real estate agencies, Centrelink (a government benefit provider) etc., as illustrated in Figure 4-8. This broad collaboration is required to properly and fully capture the fraudulent document criminal environment.

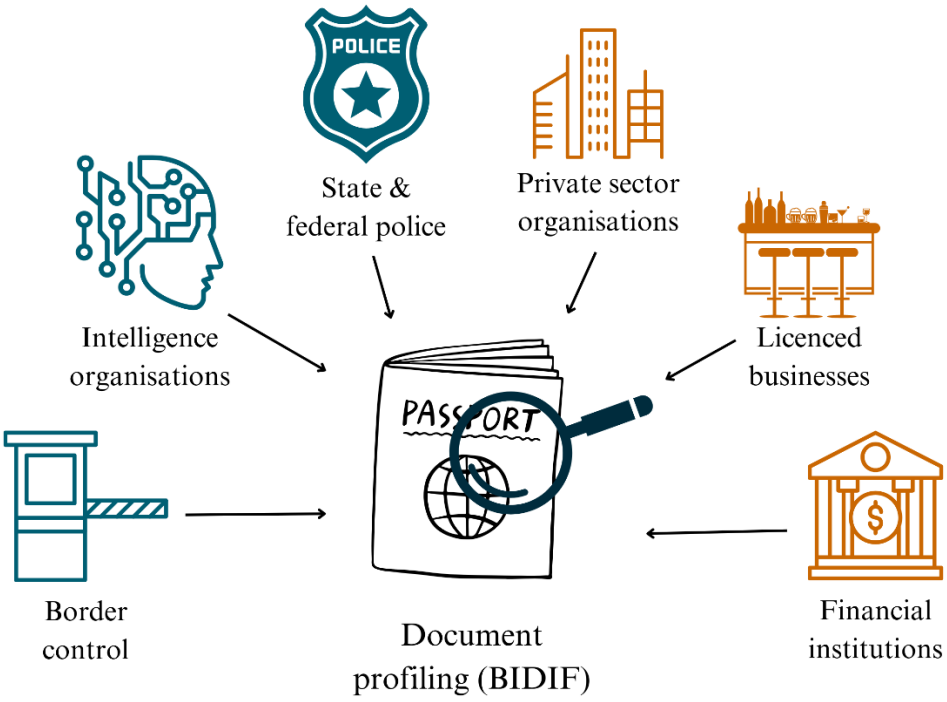


Figure 4-8: The degree of collaboration required to access the full potential that can be provided by implementing a systematic intelligence method for the profiling of fraudulent documents. The organisations here have been colour coded, with the dark teal indicating those that exist within law-enforcement, and the orange indicating those organisations that exist within the private sector but also regularly encounter identity documents.

Once the logistics of the BIDIF implementation are discussed and organised within the Australian organisations, the minor adjustments to current SOP's that are required, in

combination with the low monetary cost associated with the BIDIF/ProFID software, means that this system can be implemented quickly, and after the initial labour of incorporating the documents that are currently in storage, would simply be a manner of maintaining the system and entering documents as they are encountered. The increase in collaboration between Australian law enforcement organisations, as well as other external stake holders would be hugely beneficial, both to better understand the document fraud criminal environment, but also the overall environment of TSOC within Australia. This could generate intelligence on the tactical, strategic and operational level, providing valuable insight as well as proactively addressing the criminal environment as discussed in Section 2.1.1 as well as in Section 1.4 with examples specific to the document fraud criminal environment provided on page 51 onwards.

The implementation of BIDIF is a crucial step towards better understanding this criminal environment within Australia, and eventually internationally, but it is by no means the only thing that should be done. It is proposed that rather than relying on the traditional siloed approaches that have typically been implemented within identity crime and document fraud, that an integrated, information sharing repository is developed and implemented within Australia, as illustrated in Figure 4-9. This information sharing model would require organisations across different levels of government, the private sector, civil society, and academia to share information, whether that be reports of identity crimes, document seizures, or academic research. In combination with these already established information sources, the systematic visual profiling of fraudulent documents (such as through the incorporation of BIDIF), as well as analyses of the online market for fraudulent documents and personal information should also be incorporated.

Figure 4-9: The proposed collaborative information sharing network for identity crime and document fraud

The impacts of implementing this multi-source, forensic intelligence approach would be numerous and could assist in not only improving national policies regarding identity resilience and identity crime in general but could also support investigations into document fraud and identity crime, assist in the identification and disruption of serious and organised crime, as well

as making international collaboration more efficient, cost effective and easier. Beyond assisting in the proactive reduction of this criminal environment it also aids in making the traditional reactive policing approach more consistent across Australian states. As discussed in Chapter 1 Section 1.2.2, there are inconsistencies in identity crime related statutes across the Australian states. So, by properly examining and understanding this criminal environment, more consistent legislation could be created, thereby making the policing of this environment more consistent across Australia, paving the way towards collaboration and information sharing.

Complex and far-reaching criminal environments such as that of human trafficking cannot be addressed solely through traditional police investigation and the enforcement of federal laws. It has been noted in previous research that a broad range of fields need to be used to try and properly understand this criminal ecosystem, combining information and tactics from branches of political science, economics, social sciences, and health sciences [184, 324]. However, these different perspectives also need to be combined with the field of forensic science, and particularly forensic intelligence to assist in not just understanding the criminal environment, but to more proactively disrupt the activities of the variety of criminal networks that are involved. Incorporating police information, document profiling, research surveys, statistics, and investigations into the online market for documents and personal information, can assist even further in the identification and dismantling of these human trafficking networks.

The ability for law enforcement to properly detect, disrupt, reduce and prevent serious, transnational organised crime is largely dictated by the degree of information sharing between different organisations and countries. Currently within Australia, there are three main forms of regulated international collaboration, requests for mutual legal assistance (MLA), officers of Australian agencies going overseas to carry out specific investigative tasks, and the high-level

creation and management of cross-organisational strike teams such as the Pacific Transnational Crime Network and INTERPOL [182]. In all three cases, the monetary, time and effort costs are quite high, requiring significant organisation and investment [182, 326]. An integrated and collaborative information sharing model for identity crime provides a streamlined and much more cost and time effective way of sharing information across both domestic and international jurisdictions.

The benefits of being a part of a consistently updated and always accessible domestic and international intelligence network/memory (such as that of BIDIF and that proposed in Figure 4-9) are clear. If Australia becomes part of the international information sharing network that is integrated within BIDIF, the identification of these transnational organised crime networks would become much easier. In BIDIF, information is shared between contributing countries, while still retaining privacy, as rather than sharing full, redacted documents, the system instead shares the features of interest that have been used to classify a series. Thus, enabling the identification of international links, while still protecting sensitive information, whether that be personal or case information. BIDIF also facilitates the generation of intelligence alerts, flagging features of interest and document styles of emerging series, further enabling efficient and consistent information sharing across international partners. This can assist as well in the identification of persons of interest upon their attempted entry into the country. The use of BIDIF also requires far less time and cost investment when compared to the other international collaboration methods mentioned above.

Further, by coupling this intelligence work with the examination of the online market for fraudulent documents and personal information (as illustrated in Figure 4-3), extra scrutiny could be applied to individuals entering from countries flagged as being common suppliers of

Australian documents. This can be assisted by the integration of information from government bodies and police that handle identity crime reports. The individuals whose identity information has been compromised could help in the early identification of people illegally using their information, or information that has been sold online, to enter the country or access identity documents. The integration of the collaborative information sharing network (Figure 4-9), along with the analysis of the illicit marketplace can assist in achieving three of the four key strategies that are the foundation of the Australian response to human trafficking and slavery. These include prevention and deterrence, detection and investigation, prosecution and compliance and finally, victim support and protection [327, 328].

4.5 Recommendations

Of course, there are some hurdles that would need to be overcome before something such as this proposed model could be integrated within Australia. Outside of the general resistance towards information sharing, the culture of secrecy within Australian policing and the very strict IT security within law enforcement, the lack of priority that is given to identity crime and document fraud is a significant hurdle that needs to be overcome.

As an example, the Australian Federal Police (AFP) indicate their TSOC policing priorities to be the production and importation of drugs, money laundering, the sale of illegal firearms and dangerous goods, illegal movement across Australian borders, terrorism, human trafficking, and child exploitation [329]. These are very important areas of TSOC that do need to be targeted, but the criminal environments of identity crime and document fraud are often overlooked. Both these criminal environments need to be examined through the lens of TSOC, as research has indicated that document fraud is organised and punctuated by prolific offenders, and is known to enable, along with identity crime, other forms of serious and organised crimes [16, 32, 37, 51, 140]. In fact, all the crimes prioritised by the AFP are likely enabled by document fraud and identity crime. Therefore, by including document fraud, and by extension identity crime, within TSOC priorities, not only could an increasing criminal problem be effectively tackled, but there is the potential that these impacts would be felt in a broad range of other TSOC criminal environments as well. Thus, enabling the proactive detection, prevention and disruption of multiple criminal environments through the targeting of one trace type, such as fraudulent documents.

Only once identity crime and document fraud are included in TSOC priorities will it be possible to integrate and properly maintain an intelligence framework with consistent communication

and updates between collaborators. A first step could be the integration of BIDIF within Australian policing, starting with a domestic system first, and utilising collaboration between individual agencies that regularly encounter fraudulent documents including the police, bars, banks, border security and other relevant stakeholders. Police should be regularly checking and collecting documents from these external stakeholders, while also documenting the dates and times that they are collected to provide some basis for spatial and temporal analysis. If captured consistently (as outlined in Chapter 2 Section 2.5) these could then be logged into BIDIF and visually compared to those already in the system. This could provide greater insight into document fraud within Australia, as while the research presented in Chapter 2 suggests that the fraudulent document market is organised within Australia, a larger sample set, from a wider variety of sources needs to be examined to properly establish the structure of this criminal marketplace.

Identity crime and document fraud are rarely the end of the story as they both play an important, and often facilitative role in a range of other criminal environments. Therefore, by targeting efforts towards detecting, preventing, and disrupting identity crime and document fraud the activities of organised criminal networks and terrorist cells may be disrupted, thus impacting other TSOC criminal environments. The integration of BIDIF within Australia is the best way to illustrate the degree of organisation within the Australian market and could pave the way for further information sharing between different organisations, across different fields and eventually, internationally. This collaborative information sharing repository coupled with the integration of visual document profiling and online market analyses would create the most complete and comprehensive picture of identity crime and document fraud that there has been so far, as well as reducing the reporting burden that is placed on victims within the current identity response system [44].

4.5.1 Recommendation summary

As discussed above, the implementation of a multi-source approach to investigate and address the Australian identity crime and document fraud criminal environment has the potential to provide an array of different benefits, and a summary of the benefits, how it could be implemented and what would change for the daily operations of police and security organisations have been included in Figure 4-10.

The first step towards the information sharing network proposed in Figure 4-9 is to integrate the systematic profiling of fraudulent documents, i.e. the BIDIF system, within Australian policing (as explained in Section 2.6.1). Once this is implemented, this could pave the way for Australian policing organisations to become a part of the international BIDIF network. The success of the BIDIF implementation could garner trust between organisations, facilitate their communication and illustrate the benefits of a broader multi-approach information sharing network to better understand the document fraud and identity crime criminal environment. This would assist in the creation, implementation and maintenance of a larger information sharing repository, such as that suggested in Figure 4-9.

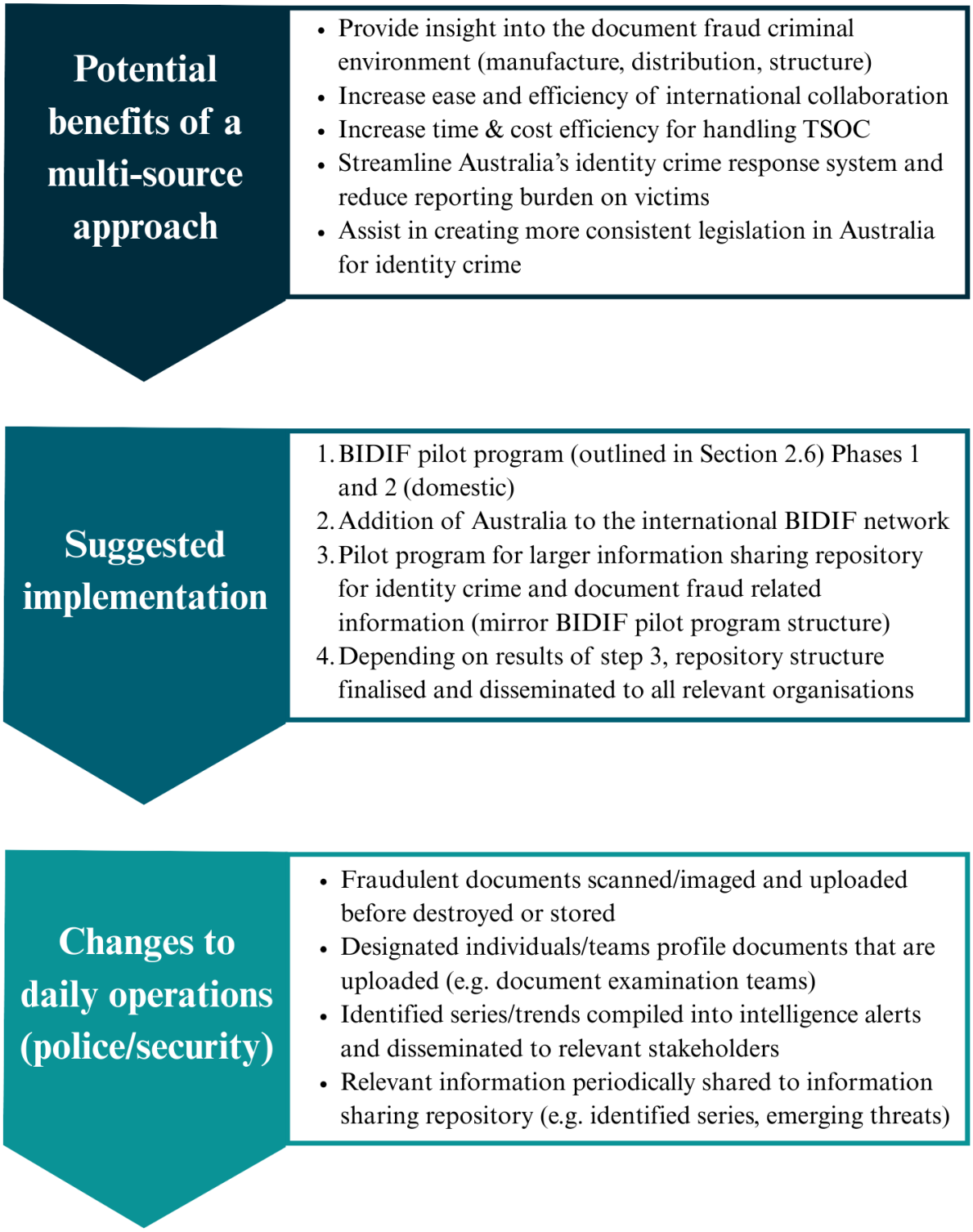


Figure 4-10: A summary of the recommendations provided in Section 4.5 along with a suggested path towards implementing the multi-source approach, as well as changes to daily operations of police and security organisations after implementation.

Conclusions and Future Directions

5 Conclusions and future directions

5.1 Conclusions

As explained in Chapter 1 and Chapter 2 Section 2.1, currently, much of the information that is gathered within the Australian identity crime and document fraud space is reliant on the reactive reporting from victims, most of which don't officially report the misuse of their personal information [29]. It is therefore crucial to shift the focus away from these solely reactive sources, and begin examining the fraudulent document criminal environment, and by extension the overarching identity crime space, in a proactive way. Internationally, the systematic profiling and comparison of fraudulent identity and travel documents has provided valuable insight into the international document market, but this area has thus far, remained relatively unexplored in Australia. Furthermore, this examination of the physical traces is only one part of the overall picture for fraudulent documents and personal information. Therefore, any attempt to understand the criminal market must be done through a combined analysis of both the physical market, being that side of the market represented by the physical traces (such as documents that are seized by police, border control and financial institutions), and the online market, being that which is facilitated through the internet.

Through the examination and profiling of 183 fraudulent documents seized from three different Australian government and law enforcement agencies, a systematic visual profiling method for Australian documents was developed, based on a published method [15] and its efficacy at detecting links between documents was illustrated. Of the documents examined, 94% of them were linked to at least one other document, with 17 series that emerged, the largest of which was of 54 documents. While the data set examined was relatively small, the results obtained here, not only illustrate that the visual profiling method works on Australian documents, in that

it identified links and series, but that the criminal environment for Australian document fraud may be organised, with prolific offenders supplying products to the market. The value of the profiling of these documents goes beyond the identification of linkages, with an analysis of the replication of security and template features providing insight into document templates and features that may be vulnerable to counterfeiting. This avenue can inform document authenticators and manufacturers what security features or templates require improvement to more effectively prevent or reduce the rate of counterfeiting. This alternative avenue of information may assist in the disruption of the criminal environment of document fraud from a different perspective, and could directly assist the Australian government in achieving one of the core goals of the National Strategy for Identity Resilience [306].

From this research, in combination with the similarities identified between the organised crime climate in both Australia and Switzerland (where ProFID and BIDIF were developed), it is clear that the BIDIF system could be implemented within Australia. Not only does this research suggest that the manual profiling method can assist in the identification of the organisation and structure within the fraudulent document market in Australia, but the semi-automated comparison portion of BIDIF, known as Padif, worked on Australian documents and it provided a useful semi-automated triaging and confirmatory aspect to the profiling method.

As the analysis of the physical fraudulent document market is only one side of the overall marketplace, in Chapter 3 an investigation into the cryptomarket facilitated portion of the online market was conducted, specifically on two cryptomarkets, WHM and Empire Market. Through the examination of sales, listings, vendor behaviours and trafficking information, this analysis suggested that the market for fraudulent documents and personal information is organised, and punctuated by prolific offenders, with a small proportion of vendors (5.5%)

contributing the majority of the products for sale (63%). While the presence of prolific offenders is not unique to the ID-related market, and is instead present across the whole cryptomarket environment, the ID-related market does seem to be more concentrated, with a higher proportion of sales being contributed by a smaller number of vendors. This was also true of the market for Australian documents, with three vendors contributing 65% of the sales within the Australian market, with all of them operating domestically.

Beyond illustrating the potential structure of the market and the presence of prolific offenders, the analysis of the online market can also provide other information to assist in intelligence-led policing. Examining the types of documents that are more commonly listed may indicate those documents and features that may be more vulnerable to counterfeiting, while also indicating routes of possible interception for physical products. The presence of domestic manufacturers within Australia suggests that more close inspections of domestic parcels may increase the detection rates of the ID-related products sold through these markets. However, this analysis has only been conducted on two cryptomarkets, with a very small proportion of physical document sales and listings, so further analysis would be required prior to outlining this as a concrete method of detection for these items.

The examination of this online portion of the market ensures that those digital products that dominate the marketplace (95% of sales on Empire) can be captured within broader analyses, as they are overlooked when focussing solely on physical traces. These products play an important role within the identity crime environment, both digital documents such as scans, as well as the personal information items, such as fullz. However, it must be remembered that the cryptomarkets examined here are only responsible for a small portion of the online ID-related market, with the sale of fraudulent documents and personal information spanning all levels of

the web. So, the harms and costs associated with this market are likely to be far higher than what has been estimated here, or in previous research. It is therefore imperative that in any illicit market analysis a multi-source approach is used, not just considering both the physical and online portions of the market, but also numerous sources from within the online market.

In Chapter 4 the online and physical portions of the market were compared, and it was found that while they share some obvious differences, they are consistent in that they are both organised and punctuated by prolific offenders. The mirroring of this structure across these two very different markets highlights the fact that they can and should be examined together as two parts of the same whole. To properly understand the market for fraudulent documents and personal information, the supply chain of these products needs to be interrogated, examining where they have come from along with how they have been manufactured and distributed. The analysis of this supply chain not only increases the understanding of the criminal environment overall but can also create opportunities for earlier interception of these documents, prior to them being used to enable or facilitate a criminal offence (which is when they are most often detected).

But the analysis of the illicit marketplace in isolation is not sufficient to understand this complex criminal environment. As has been recommended to assist in the understanding of other illicit markets, such as that for illicit drugs [96-98], this work has proposed a multi-source interdisciplinary approach towards identity crime and document fraud, incorporating information from police, the visual profiling of fraudulent documents, identity crime reporting systems, the private sector, and online market analyses, along with surveys and statistics. It is suggested that all these traditionally separate organisations should work collaboratively to create and maintain an information sharing network that is consistently updated to provide

relevant intelligence and information about the identity crime and document fraud criminal environment. The pervasive and prolific crime problem that is identity crime and document fraud has given no indication that it will slow down in the coming years. The increases in digital technologies and the amount of personal information being stored online is creating the perfect storm in which identity crime and document fraud can flourish.

The research conducted here clearly illustrates that the current understanding of the criminal environments for document fraud and identity crime is hampered by the reliance on the reactive approach. Only through a multi-source approach, built upon broad collaborations and information sharing across all relevant stakeholders, can there be long lasting and meaningful impact upon this criminal environment, as well as other criminal environments that document fraud is known to enable.

5.2 Future directions

This work aimed to develop a holistic understanding of the criminal environment of identity crime and document fraud and to subsequently propose a multi-source approach to facilitate its more proactive disruption within an intelligence-led policing paradigm. Along the way to achieving this overarching goal, a systematic intelligence method for the profiling of fraudulent documents, as well as regular analyses of online markets selling and distributing fraudulent documents and personal information should be considered. In this section, the future directions have been divided by chapter.

5.2.1 The forensic profiling of fraudulent identity documents

The current research had a very strong focus on Australian driver licences, and while these were selected as the document of interest based on the ease of access, expanding the document set to consider different document types, as well as international documents will provide valuable, additional information. This is especially important when considering passports, as counterfeit passports, both international and domestic, are a point of interest for law enforcement organisations, particularly those that are focussed on policing the borders. As illustrated in this work, the profiling and comparison of international documents is a worthwhile avenue of interest, with these documents leading to potential international links. These links could assist in the identification of organised criminal networks in Australia.

The work conducted here is only a small snapshot of the fraudulent document criminal environment, as the documents examined were from only three law enforcement organisations, all of which were located on the Eastern side of Australia. Given the level of organisation and structure identified within the documents examined here, it is of great interest to investigate whether this organisation is present across the national canvas, and to what level. If the method

was expanded to include and consider documents that were intercepted by a range of organisations, including those such as banks and others that regularly authenticate documents, a far better picture of this criminal environment would be created, adding to the valuable information outlined within this research. Furthermore, if more contextual information was gathered around the documents, more in depth social network analysis could be conducted, and if a known source seizure was intercepted, this could enable and interrogation of the social networks of the known source.

5.2.1.1 Consideration of digital documents

As information and digital technologies have been increasing, there has been the implementation of more digital proof of identity documents, such as the digital driver licence (DDL) implemented in NSW in late 2019. While it is hypothesised that physical documents will always have a role within proof of identity processes [51], it is inevitable that there will gradually be more and more digital documents implemented, with society likely moving towards a blended identity proof approach, incorporating a combination of both digital and physical documents [51]. It is therefore important that the profiling method that has been developed for physical documents also be applicable to documents that are housed within a digital space. The profiling method is versatile, in that it can be applied to any document that contains visual elements; however, difficulties can be introduced when dealing with a document that appears legitimate, in that the security features have been successfully replicated.

Specifically in relation to the NSW digital driver licence (DDL), police have indicated that there have been instances of underage individuals editing a screenshot or still of the DDL. These were considered as potential items of interest for the research conducted here, however,

the images of these licences were of too low a quality to be compared (often being a photo of a phone screen). Even if the images were of a high quality, a visual comparison between these digital documents would be limited, especially if the individuals were simply editing the documents themselves using paint, GIMP or the like. However, a different avenue of interest presents itself when considering the potential to "hack" the digital driver licences. Recent news publications have indicated that the digital drivers licence can be hacked, with fraudsters illegally accessing legitimate documents that they then edit, circumventing the security measures [330]. While not possible to profile these digital documents visually, as they appear legitimate, there is the potential of using digital forensic science to conduct examinations on the digital traces left on these documents, within the application through which the document is accessed.

The value of implementing more collaborations between digital forensic science and document examination is clear when considering the emergence of AI counterfeit documents as discussed in Chapter 4 Section 4.2. This is another instance in which shifting focus to consider the digital traces of these images could provide valuable insight into their supply chain. With this increasing emergence of digital identity documents, it may be of interest to consider integrating analysis of image meta data and other digital traces into the BIDIF system that is already being used. It would be worthwhile to consider how these purely digital counterfeit documents could be integrated within BIDIF, incorporating their meta data as well as the images themselves to enable comparison and examination of the combination of their different traces.

5.2.2 The investigation of the online Australian document market

As the cryptomarket criminal problem is so pervasive and prolific, there is never any shortage of active markets that can be crawled and used to provide insight into the cryptomarket

facilitated portion of any illicit marketplace. To continue to gain insight into the ID-related market, and by extension the criminal environment of identity crime, more cryptomarkets need to be examined, to not only increase the understanding of this marketplace, but to get a better cross-section of the products that are being listed and sold as well as the different vendors that are operating.

This examination should also extend to markets and vendors on the dark web that exist outside the jurisdiction of the cryptomarkets, including those with independent store fronts, and operating in the other levels of the web including storefront, forums and messaging applications such as Telegram [304]. Furthermore, as clearly illustrated by the comparison between the pseudo documents seized by NSWPF and those that were being supplied by the online vendor, the open web is a source of documents for customers in Australia. This was just one of many open web store fronts for fraudulent documents, so these vendors need to be considered in any analysis of this illicit marketplace.

The continuous monitoring of this side of the marketplace is required to stay on top of emerging trends in the market, both regarding fraudulent documents and personal information, as this monitoring could assist in the identification of data breaches, or vulnerable information security measures that has led to the theft of personal information. Furthermore, it can assist in informing on any changes in vendors of interest, i.e. those that are performing at a high rate, and could therefore assist in the potential identification of those that are significant contributors to the market.

As has been conducted in Switzerland, on illicit drug products [331], the purchase of some of the ID-related products listed on these markets would facilitate a comparison between the product listings, and the items that the buyer receives. The purchase of both digital and physical

documents as well as items within the identity fraud related category would provide insight into the accuracy of the vendors listings, as well as how these items are manufactured, information that was targeted, and techniques that are used in their creation. It could also provide insight into the shipping and packaging methods used, as well as the reliability of vendors of interest.

The online space holds a mass of potential information about the market for fraudulent documents and personal information, that so far has been underutilised from an intelligence perspective. Consistent and regular monitoring of this space can provide valuable information and intelligence about the supply chain of these products, and can assist in the proactive reduction, disruption, and prevention of this criminal environment.

5.2.3 The multi-source approach for document fraud and identity crime

The most value that can be gained from the analysis of the physical and online portions of the market arises through their combined analysis within a multi-source approach. Combining regular profiling and comparison of document seizures, with regular online market analyses (as shown in Figure 4-3) could provide clear timelines of trends in manufacture and distribution and would provide a clearer illustration of the links between the online and physical portions of the market. This could be furthered by conducting active comparisons between documents purchased from vendors of interest and those that are being intercepted by law enforcement agencies within Australia.

On an organisational level, implementing something like the integrated information sharing network proposed in Chapter 4 will have significant challenges, largely due to the culture of secrecy and lack of information sharing that has become standard within Australian policing and government organisations [198]. To break the culture of secrecy, partnerships need to be

established, nurtured and maintained to create trust between different organisations and if there is to be any hope of implementing a multi-source approach such as that proposed, the foundations for these partnerships need to start being built now.

This will be no mean feat, but the most logical first step towards the end goal of this overall multi-source approach would be the implementation of ProFID/BIDIF within Australian policing. Given the design of the ProFID system, its ability to ease the information sharing process while still protecting sensitive information, and the clear success of the method on Australia documents, it would be a good illustration of the power of information sharing and collaboration within the identity crime and document fraud environment.

It is recommended that the implementation of BIDIF could be a first step, on a domestic level at first to trial the information sharing and collaboration between law enforcement agencies, border security and the public sector. This would also serve to provide better understanding regarding the size and structure of the fraudulent document market in Australia on a more realistic scale, informing on the best way to implement and maintain the larger information sharing network that has been proposed in this chapter. In a criminal environment that is advancing with leaps and bounds alongside increases in technology and the amount of information provided online, more effort, resources and collaboration is required to properly understand and therefore prevent and disrupt the criminal environment of identity crime and document fraud. If the required advancements are not made, police and law enforcement will continue to be stuck, spinning their wheels in the mud, trying to catch up and manage this escalating problem.

References

References

1. Morelato, M., et al., (2014), Forensic intelligence framework-Part I: Induction of a transversal model by comparing illicit drugs and false identity documents monitoring. *Forensic Science International*, **236**(C): p. 181-190, 10.1016/j.forsciint.2013.12.045.
2. Ribaux, O., et al., (2010), Intelligence-led crime scene processing. Part I: Forensic intelligence. *Forensic Science International*, **195**(1-3): p. 10-16, 10.1016/j.forsciint.2009.10.027.
3. Ribaux, O., et al., (2010), Intelligence-led crime scene processing. Part II: Intelligence and crime scene examination. *Forensic Science International*, **199**(1-3): p. 63-71, 10.1016/j.forsciint.2010.03.011.
4. Ribaux, O., et al., *Forensic Intelligence*, in *Encyclopedia of Forensic Sciences*, J.A. Siegel, P.J. Saukko, and M.M. Houck, Editors. 2013. p. 298-302.
5. Ratcliffe, J.H. and R. Guidetti, (2008), State police investigative structure and the adoption of intelligence-led policing. *Policing: An International Journal of Police Strategies & Management*, **31**(1): p. 109-128, 10.1108/13639510810852602.
6. Weisburd, D. and J.E. Eck, (2004), What Can Police Do to Reduce Crime, Disorder, and Fear? *The Annals of the American Academy of Political and Social Science*, **593**(1): p. 42-65, 10.1177/0002716203262548.
7. Morelato, M., et al., (2013), The use of forensic case data in intelligence-led policing: The example of drug profiling. *Forensic Science International*, **226**(1): p. 1-9, https://doi.org/10.1016/j.forsciint.2013.01.003.
8. Ribaux, O., F. Crispino, and C. Roux, (2015), Forensic intelligence: deregulation or return to the roots of forensic science? *Australian Journal of Forensic Sciences*, **47**(1): p. 61-71, 10.1080/00450618.2014.906656.
9. Ribaux, O. and B. Talbot Wright, (2014), Expanding forensic science through forensic intelligence. *Science & Justice*, **54**(6): p. 494-501, https://doi.org/10.1016/j.scijus.2014.05.001.
10. Ribaux, O., S.J. Walsh, and P. Margot, (2006), The contribution of forensic science to crime analysis and investigation: Forensic intelligence. *Forensic Science International*, **156**(2-3): p. 171-181, 10.1016/j.forsciint.2004.12.028.
11. Baechler, S., R. Boivin, and P. Margot, (2015), Systematic processing of false identity documents for crime intelligence purposes: Towards a systematic approach. *Revue Internationale de Criminologie et de Police Technique et Scientifique*, **68**(C): p. 315-337,
12. Baechler, S., et al., (2011), False identity documents profiling: A promising forensic intelligence method to fight identity document fraud. *Revue Internationale de Criminologie et de Police Technique et Scientifique*, **64**(4): p. 467-480,
13. Baechler, S. and P. Margot, (2016), Understanding crime and fostering security using forensic science: The example of turning false identity documents into forensic intelligence. *Security Journal*, **29**(4): p. 618-639, 10.1057/sj.2015.26.
14. Baechler, S., et al., (2015), Forensic intelligence framework. Part II: Study of the main generic building blocks and challenges through the examples of illicit drugs and false identity documents monitoring. *Forensic Science International*, **250**(C): p. 44-52, https://doi.org/10.1016/j.forsciint.2015.02.021.
15. Baechler, S., O. Ribaux, and P. Margot, (2012), 2012 Student Paper: Toward a Novel Forensic Intelligence Model: Systematic Profiling of False Identity Documents.

Forensic Science Policy & Management: An International Journal, **3**(2): p. 70-84, 10.1080/19409044.2012.744120.
16. Baechler, S., et al., (2013), The systematic profiling of false identity documents: Method validation and performance evaluation using seizures known to originate from common and different sources. *Forensic Science International*, **232**(1): p. 180-190, 10.1016/j.forsciint.2013.07.022.
17. Moulin, S.L., C. Weyermann, and S. Baechler, (2022), An efficient method to detect series of fraudulent identity documents based on digitised forensic data. *Science & Justice*, **62**(5): p. 610-620, 10.1016/j.scijus.2022.09.003.
18. Mireault, C., et al., (2017), What if counterfeit IDs could talk ? Chemical profiling of identity documents. *Keesing Journal of Documents & Identity*: p. 9-12,
19. Talbot-Wright, B., et al., (2016), Image processing of false identity documents for forensic intelligence. *Forensic Science International*, **263**(C): p. 67-73, 10.1016/j.forsciint.2016.03.054.
20. Farrar, J.H., (2011), Fighting Identity Crime. *Bond Law Review*, **23**(1),
21. Ahmed, S.R., (2020), *Preventing Identity Crime: An Identity Crime Model and Legislative Analysis with Recommendations for Preventing Identity Crime, (1st),* Brill.
22. Department of Home Affairs,, (2016), *National Identity Proofing Guidelines, https://www.homeaffairs.gov.au/criminal-justice/files/national-identity-proofing-guidelines.pdf*
23. Koops, B.-J., et al., (2009), A Typology of Identity-Related Crime. *Information, Communication & Society*, **12**(1): p. 1-24, 10.1080/13691180802158516.
24. United Kingdom Cabinet Office, (2002), *Identity Fraud: A Study,* http://www.statewatch.org/news/2004/may/id-fraud-report.pdf
25. Ombelli, D. and F. Knopjes, (2008), *Documents: The Developer's Toolkit,* Via Occidentalis.
26. About, I. and V. Denis, (2010), *Histoire de l'identification des personnes,* La Découverte.
27. Fahrmeir, A., *Government and forgers: passports in nineteenth-century Europe*, in *Documenting Individual Identity*, J. Caplan and J. Torpey, Editors. 2001, Princeton University Press: Princeton.
28. Groebner, V., (2007), *Who are you? Identification, deception, and surveillance in early modern Europe,* Zone Books.
29. Franks, C. and R. Smith, (2020), *Identity crime and misuse in Australia 2019,*
30. McAlister, M., et al., (2023), *Identity crime and misuse in Australia 2023,* A. Government,
31. McAlister, M. and C. Franks, (2021), *Identity crime and misuse in Australia: Results of the 2021 online survey,* https://doi.org/10.52922/sb78467
32. Europol,, (2017), *European Union serious and organised crime threat assessment: Crime in the age of technology, https://www.europol.europa.eu/activities-services/main-reports/european-union-serious-and-organised-crime-threat-assessment-2017*
33. The Australasian Centre for Policing Research (ACPR),, (2006), *Standardisation of definitions of identity crime terms: A step towards consistency, https://static.aminer.org/pdf/PDF/000/246/496/electronic_commerce_fraud_towards_an_understanding_of_the_phenomenon.pdf*

34. Steel, A., (2010), The True Identity of Australian Identity Theft Offences: A Measured Response or an Unjustified Status Offence? *University of New South Wales Law Journal*, **33**: p. 503-531,
35. Golladay, K. and K. Holtfreter, (2017), The Consequences of Identity Theft Victimization: An Examination of Emotional and Physical Health Outcomes. *Victims & Offenders*, **12**(5): p. 741-760, 10.1080/15564886.2016.1177766.
36. G8 Lyon-Roma Anti-Crime and Terrorism Group. Criminal and Legal Affairs Subgroup, (2009), *Essential Elements of Criminal Laws to Address Identity-related Crime,*
37. Europol, (2021), *European Union serious and organised crime threat assessment, A corrupting influence: the infiltration and undermining of Europe's economy and society by organised crime, https://www.europol.europa.eu/activities-services/main-reports/european-union-serious-and-organised-crime-threat-assessment*
38. Frontex Risk Analysis Unit, (2019), *Risk analysis for 2019,* https://frontex.europa.eu/publications/risk-analysis-for-2019-RPPmXE
39. Friedrich, E., (2001), Fälschungskriminalität und Prävention - Sicherungstechnische Anforderungen an Ausweisdokumente. *Kriminalistik*, **55**(4): p. 271-277,
40. INTERPOL, (2019), *Identity and travel document fraud, https://www.interpol.int/ar/content/download/10479/file/Identity%20and%20travel%20document%20fraud.pdf*
41. Levinson, J., (1984), Passport Examination. *Journal of Forensic Sciences*, **29**(2): p. 628-632, 10.1520/JFS11715J.
42. Pfefferli, P.W., *Forgery/Counterfeits*, in *Encyclopedia of Forensic Sciences*, J.A. Siegel, Editor. 2000, Elsevier: Oxford. p. 580-584.
43. Trubshoe, T. and J. McGinn, *Forgery/Counterfeits*, in *Encyclopedia of Forensic Sciences (Second Edition)*, J.A. Siegel, P.J. Saukko, and M.M. Houck, Editors. 2013, Academic Press: Waltham. p. 360-366.
44. Wyre, M., D. Lacey, and K. Allan, (2020), *The identity theft response system,* https://www.aic.gov.au/sites/default/files/2020-05/ti592_the_identity_theft_response_system.pdf
45. Prenzler, T., *Fraud victimisation and prevention*, in *The Australian and New Zealand handbook of criminology, crime and justice*, A. Deckert and R. Sarre, Editors. 2017, Routledge: London. p. 269-283.
46. Australian Competition and Consumer Commission (ACCC), (2022), *Targeting scams: Report of the ACCC on scams activity 2022,* https://www.accc.gov.au/system/files/Targeting%20scams%202022.pdf
47. Jorna, P. and R.G. Smith, (2017), *Identity crime and misuse in Australia 2017,* https://www.aic.gov.au/publications/sr/sr10
48. Commonwealth of Australia, (2024), *IDMatch,* https://www.idmatch.gov.au/
49. Information and privacy commission (IPC), (2007), *Direction relating to the document verification service - NSW Roads and Traffic Authority,* https://www.ipc.nsw.gov.au/direction-relating-document-verification-service-nsw-roads-and-traffic-authority
50. Deviterne-Lapeyre, M. and S. Ibrahim, (2023), Interpol questioned documents review 2019–2022. *Forensic Science International: Synergy*, **6**: p. 100300, https://doi.org/10.1016/j.fsisyn.2022.100300.

51. Baechler, S., (2020), Document Fraud: Will Your Identity Be Secure in the Twenty-first Century? *European Journal on Criminal Policy and Research*, **26**(3): p. 379-98, 10.1007/s10610-020-09441-8.
52. Organisation for Security and Co-operation in Europe (OSCE), (2017), *Intelligence-Led Policing,* OSCE Secretariat.
53. Ratcliffe, J.H., (2003), Intelligence-led Policing. *Trends & Issues in Crime and Criminal Justice*, (248): p. 1-6,
54. Bradley, D., *Escaping Plato's cave*, in *Policing Australia: Old issues, new perspectives*, P. Moir and H. Eijkman, Editors. 1992, Palgrave Macmillan: Melbourne.
55. Drew, J. and T. Prenzler, (2015), *Contemporary Police Practice,* Oxford University Press.
56. Grabosky, P., (2007), The Internet, Technology, and Organized Crime. *Asian Journal of Criminology*, **2**(2): p. 145-161, 10.1007/s11417-007-9034-z.
57. Audit Commission, (1993), *Audit Commission Helping with Enquiries: Tackling Crime Effectively,*
58. Ratcliffe, J.H., (2008), *Intelligence-Led policing,* Willan Publishing.
59. National Criminal Intelligence Service (NCIS),, (2000), *The National Intelligence Model,*
60. Ratcliffe, J.H., (2016), *Intelligence-Led Policing, (2nd),* Routledge.
61. Innes, M., N. Fielding, and N. Cope, (2005), The Appliance of Science: The Theory and Practice of Crime Intelligence Analysis. *The British Journal of Criminology*, **45**(1): p. 39-57, 10.1093/bjc/azh053.
62. Wiggett, A.E., et al., (2003), Forensic Science Society Spring Meeting 2002 Intelligence. *Science & Justice*, **43**(2): p. 109-118, https://doi.org/10.1016/S1355-0306(03)71752-3.
63. Coyne, J.W. and P. Bell, (2011), The role of strategic intelligence in anticipating transnational organised crime: A literary review. *International Journal of Law, Crime and Justice*, **39**(1): p. 60-78, https://doi.org/10.1016/j.ijlcj.2011.02.003.
64. Ratcliffe, J.H., (2007), *Integrated Intelligence and Crime Analysis: Enhanced Information Management for Law Enforcement Leaders,* Police Foundation, United States of America.
65. Cartier, J., (2009), *La recherche et la gestion des liens dans l'investigation criminelle: le cas de la criminalité organisée*, (Doctoral), Université de Lausanne, Lausanne, Switzerland.
66. Glass, R.R. and P.B. Davidson, (1948), *Intelligence is for Commanders,* Military Service Publishing Company.
67. Phythian, M., (2013), *Understanding the intelligence cycle,* Routledge.
68. Peterson, M., (2005), *Intelligence-led Policing: The New Intelligence Architecture,*
69. Aepli, P., E. Summerfield, and O. Ribaux, (2011), *Decision Making in Policing,* EFPL Press.
70. Cusson, M., B. Dupont, and F. Lemieux, (2008), *Traité de sécurité intérieure,* Presses Polytechniques et Universitaires Romandes (PPUR).
71. Forensic Intelligence (FORINT) Specialist Advisory Group, (2022), *Forensic Intelligence Lexicon,* https://www.anzpaa.org.au/ArticleDocuments/346/Forensic%20Intelligence%20Lexicon.PDF.aspx

72. United Nations Office on Drugs and Crime (UNODC),, (2011), *Criminal intelligence: Manual for analysts, https://www.unodc.org/documents/organized-crime/Law-Enforcement/Criminal_Intelligence_for_Analysts.pdf*
73. Cope, N., (2004), 'Intelligence Led Policing or Policing Led Intelligence?': Integrating Volume Crime Analysis into Policing. *The British Journal of Criminology*, **44**(2): p. 188-203, 10.1093/bjc/44.2.188.
74. Legrand, T. and L. Vogel, (2015), The landscape of forensic intelligence research. *Australian Journal of Forensic Sciences*, **47**(1): p. 16-26, 10.1080/00450618.2014.928830.
75. Walsh, S.J., et al., (2008), Comparing the growth and effectiveness of forensic DNA databases. *Forensic Science International: Genetics Supplement Series*, **1**(1): p. 667-668, https://doi.org/10.1016/j.fsigss.2007.11.011.
76. De Ceuster, J., et al., (2012), A discussion on the usefulness of a shared European ballistic image database. *Science & Justice*, **52**(4): p. 237-242, https://doi.org/10.1016/j.scijus.2011.12.003.
77. Rossy, Q., et al., (2013), Integrating forensic information in a crime intelligence database. *Forensic Science International*, **230**(1): p. 137-146, https://doi.org/10.1016/j.forsciint.2012.10.010.
78. Walsh, S.J., J.M. Curran, and J.S. Buckleton, (2010), Modeling forensic DNA database performance. *Journal of Forensic Sciences*, **55**(5): p. 1174-83, 10.1111/j.1556-4029.2010.01426.x.
79. Taylor, M.L., et al., (2024), Forensic intelligence in Australia and New Zealand: Status and future directions. *Forensic Science International*, **364**: p. 112207, https://doi.org/10.1016/j.forsciint.2024.112207.
80. Ratcliffe, J.H., (2002), Intelligence-led policing and the problems of turning rhetoric into practice. *Policing and Society*, **12**(1): p. 53-66, 10.1080/10439460290006673.
81. Ribaux, O. and T. Hicks, *Technology and database expansion: What impact on policing?*, in *Technocrime: Policing and Surveillance*, S. Leman-Langlois, Editor. 2013, Routledge: United Kingdom. p. 91-109.
82. Broséus, J., et al., (2016), Chemical profiling: A tool to decipher the structure and organisation of illicit drug markets: An 8-year study in Western Switzerland. *Forensic Science International (Online)*, **266**(C): p. 18-28, http://dx.doi.org/10.1016/j.forsciint.2016.04.008.
83. Marquis, R., et al., (2008), Drug intelligence based on MDMA tablets data: 2. Physical characteristics profiling. *Forensic Science International*, **178**(1): p. 34-39, https://doi.org/10.1016/j.forsciint.2008.01.014.
84. Weyermann, C., et al., (2008), Drug intelligence based on MDMA tablets data: I. Organic impurities profiling. *Forensic Science International*, **177**(1): p. 11-16, https://doi.org/10.1016/j.forsciint.2007.10.001.
85. Esseiva, P., et al., (2003), A methodology for illicit heroin seizures comparison in a drug intelligence perspective using large databases. *Forensic Science International*, **132**(2): p. 139-152, https://doi.org/10.1016/S0379-0738(03)00010-0.
86. Been, F., et al., (2011), Profiling of counterfeit medicines by vibrational spectroscopy. *Forensic Science International*, **211**(1): p. 83-100, https://doi.org/10.1016/j.forsciint.2011.04.023.

87. Dégardin, K., et al., (2018), Packaging analysis of counterfeit medicines. *Forensic Science International*, **291**: p. 144-157, https://doi.org/10.1016/j.forsciint.2018.08.023.
88. Dégardin, K., Y. Roggo, and P. Margot, (2015), Forensic intelligence for medicine anti-counterfeiting. *Forensic Science International*, **248**: p. 15-32, http://dx.doi.org/10.1016/j.forsciint.2014.11.015.
89. Hochholdinger, S., et al., (2019), Elemental analysis for profiling counterfeit watches. *Forensic Science International*, **298**: p. 177-185, 10.1016/j.forsciint.2019.03.006.
90. Bruenisholz, E., et al., (2017), Repetitive deliberate fires: Development and validation of a methodology to detect series. *Forensic Science International*, **277**: p. 148-160, https://doi.org/10.1016/j.forsciint.2017.06.009.
91. Agius, A., et al., (2018), Using handwriting to infer a writer's country of origin for forensic intelligence purposes. *Forensic Science International (Online)*, **282**: p. 144-156, http://dx.doi.org/10.1016/j.forsciint.2017.11.028.
92. Auberson, M., et al., (2016), Development of a systematic computer vision-based method to analyse and compare images of false identity documents for forensic intelligence purposes-Part I: Acquisition, calibration and validation issues. *Forensic Science International*, **260**: p. 74-84, 10.1016/j.forsciint.2016.01.016.
93. Ribaux, O., (2023), *De la police scientifique à la traçologie, (Second),* EPFL Press.
94. United Nations Office on Drugs and Crime (UNODC), (2018), *World drug report 2018,*
95. Department of Health,, (2017), *National Drug Strategy 2017-2026, https://www.health.gov.au/resources/collections/national-drug-strategy*
96. Morelato, M., et al., (2018), Forensic drug intelligence and the rise of cryptomarkets. Part II: Combination of data from the physical and virtual markets. *Forensic Science International*, **288**: p. 201-210, 10.1016/j.forsciint.2018.05.002.
97. Zobel, F., et al., (2017), *Le marché des stupéfiants dans le canton de Vaud: Les opioïdes,* https://www.addictionsuisse.ch/fileadmin/user_upload/Rapport_MARSTUP_1.pdf
98. Zobel, F., et al., (2018), *Le marché des stupéfiants dans le canton de Vaud. Partie 2: Cocaïne et autres stimulants,* https://serval.unil.ch/resource/serval:BIB_354941DEC8D2.P001/REF.pdf
99. Morelato, M., et al., (2019), When does the cutting of cocaine and heroin occur? The first large-scale study based on the chemical analysis of cocaine and heroin seizures in Switzerland. *International Journal of Drug Policy*, **73**: p. 7-15, 10.1016/j.drugpo.2019.07.025.
100. Ioset, S., et al., (2005), Establishment of an operational system for drug profiling: A Swiss experience. *Bulletin on Narcotics*, **57**(1-2): p. 121-47,
101. Morelato, M., et al., (2014), The use of organic and inorganic impurities found in MDMA police seizures in a drug intelligence perspective. *Science & Justice*, **54**(1): p. 32-41, https://doi.org/10.1016/j.scijus.2013.08.006.
102. Popovic, A., et al., (2022), Understanding Australian methylamphetamine drug markets through relational, temporal and spatial analyses. *Drug Testing and Analysis*, **14**(3): p. 481-495, 10.1002/dta.3181.
103. Aldridge, J. and D. Décary-Hétu, (2016), Hidden Wholesale: The drug diffusing capacity of online drug cryptomarkets. *The International Journal of Drug Policy*, **35**: p. 7-15, 10.1016/j.drugpo.2016.04.020.

104. Broséus, J., et al., (2017), Forensic drug intelligence and the rise of cryptomarkets. Part I: Studying the Australian virtual market. *Forensic Science International (Online)*, **279**: p. 288-301, http://dx.doi.org/10.1016/j.forsciint.2017.08.026.
105. Cunliffe, J., et al., (2017), An island apart? Risks and prices in the Australian cryptomarket drug trade. *The International Journal of Drug Policy*, **50**: p. 64-73, 10.1016/j.drugpo.2017.09.005.
106. Demant, J., et al., (2019), Going local on a global platform: A critical analysis of the transformative potential of cryptomarkets for organized lllicit drug crime (vol 28, pg 255, 2018). *International Criminal Justice Review*, **29**(4): p. 386-386, 10.1177/1057567718784445.
107. Dolliver, D.S. and J.L. Kenney, (2016), Characteristics of Drug Vendors on the Tor Network: A Cryptomarket Comparison. *Victims & Offenders*, **11**(4): p. 600-620, 10.1080/15564886.2016.1173158.
108. Man, N., et al., (2021), *Trends in the availability and type of drugs sold on the internet via cryptomarkets, January 2020 - Janauary 2021,* S. University of New South Wales (UNSW), chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://ndarc.med.unsw.edu.au/sites/default/files/ndarc/resources/DNeT-bulletin-Jan2020-Jan2021_0.pdf
109. Moeller, K., R. Munksgaard, and J. Demant, (2017), Flow My FE the Vendor Said: Exploring Violent and Fraudulent Resource Exchanges on Cryptomarkets for Illicit Drugs. *American Behavioral Scientist*, **61**(11): p. 1427-1450, 10.1177/0002764217734269.
110. Van Buskirk, J., et al., (2016), Who sells what? Country specific differences in substance availability on the Agora cryptomarket. *The International Journal of Drug Policy*, **35**: p. 16-23, 10.1016/j.drugpo.2016.07.004.
111. Batistic, F.-K., et al., (2021), Analysis of Google Trends to monitor new psychoactive substance. Is there an added value? *Forensic Science International*, **326**, 10.1016/j.forsciint.2021.110918.
112. Rhumorbarbe, D., et al., (2019), Monitoring new psychoactive substances: Exploring the contribution of an online discussion forum. *International Journal of Drug Policy*, **73**: p. 273-280, 10.1016/j.drugpo.2019.03.025.
113. Bannwarth, A., et al., (2019), The use of wastewater analysis in forensic intelligence: drug consumption comparison between Sydney and different European cities. *Forensic Sciences Research*, **4**(2): p. 141-151, 10.1080/20961790.2018.1500082.
114. Puljevic, C., et al., (2024), Characterising differences between self-reported and wastewater-identified drug use at two consecutive years of an Australian music festival. *The Science of the Total Environment*, **921**: p. 170934, 10.1016/j.scitotenv.2024.170934.
115. Fursman, H., et al., (2024), A snapshot of injecting drug consumption from the analysis of used syringes within the Medically Supervised Injecting Centre in Sydney, Australia. *Drug and Alcohol Review*, **43**(3): p. 787-798, 10.1111/dar.13803.
116. Lefrancois, E., et al., (2020), Substances injected at the Sydney supervised injecting facility: A chemical analysis of used injecting equipment and comparison with self-reported drug type. *Drug and Alcohol Dependence*, **209**, 10.1016/j.drugalcdep.2020.107909.

117. Broséus, J., et al., (2017), A geographical analysis of trafficking on a popular darknet market. *Forensic Science International (Online)*, **277**: p. 88-102, http://dx.doi.org/10.1016/j.forsciint.2017.05.021.
118. Clarke, C.P., (2016), Drugs & Thugs: Funding Terrorism through Narcotics Trafficking. *Journal of Strategic Security*, **9**(3): p. 1-15, 10.5038/1944-0472.9.3.1536.
119. Deviterne-Lapeyre, C.M., (2020), Interpol review of questioned documents 2016–2019. *Forensic Science International: Synergy*, https://doi.org/10.1016/j.fsisyn.2020.01.012.
120. Mathyer, J., (1980), Some remarks on the problem of the security of identity documents: an interesting solution. *Revue Internationale de Police Criminelle*, **35**(336): p. 66-79,
121. Amjed, A., B. Mahmood, and K.A.K. Almukhtar. *Approaches for Forgery Detection of Documents in Digital Forensics: A Review*. in *International Conference on Emerging Technology Trends in Internet of Things and Computing*. 2022. Erbil, Iraq: Springer International Publishing.
122. Bibi, M., et al., (2022), Document forgery detection using source printer identification: A comparative study of text-dependent versus text-independent analysis. *Expert Systems*, **39**(8): p. n/a, 10.1111/exsy.13020.
123. Weyermann, C., et al., (2023), Towards more relevance in forensic science research and development. *Forensic Science International*: p. 111592, https://doi.org/10.1016/j.forsciint.2023.111592.
124. Pfefferli, P.W., (2001), *Review 1998-2001 from the Coordinating Laboratory on questioned documents (other than handwriting)* [Conference paper],13th International Forensic Science Symposium,Lyon, France,
125. Angstrom, N. *Questioned documents - A review: 2001 to 2004*. in *14th International Forensic Science Symposium*. 2004. Lyon, France: Interpol.
126. Fritz, T., (2007), *Questioned documents - A review: 2004 to 2007* [Conference paper],15th International Forensic Science Symposium,Lyon, France,
127. Fritz, T., (2010), *Examination of questioned documents/handwriting - review: 2007 to 2010* [Conference paper],16th International Forensic Science Symposium,Lyon, France,
128. Partouche, F. *Questioned documents - Review 2010-2013*. in *17th International Forensic Science Managers Symposium.* 2013. Lyon.
129. Morton, S.E., (1984), Counterfeits: Three groups, one source. *Journal of Forensic Sciences*, **29**(1): p. 310-316, 10.1520/jfs11665j.
130. Pfefferli, P.W., et al., (1999), Bekämpung von Ausweis- und Visums-fälschungen : ein Lagebericht. *Kriminalistik*, **53**: p. 833,
131. Ng, P.K., et al., (2004), Methods of forgery in counterfeit travel documents. *Journal of the American Society of Questioned Document Examiners*, **7**(2): p. 83-90,
132. Estabrooks, C., et al., (2004), Authentication of travel documents via the imagexpert system. *Journal of the American Society of Questioned Document Examiners*, **7**(2): p. 97-104,
133. United Nations Office on Drugs and Crime (UNODC),, (2010), *Report of observations and conclusions of the session on the use of forensic sciences to combat and prevent identity-related crime,*
134. Gordon, G.R., (2003), *Identity Fraud: A Critical National and Global Threat,*

135. Europol, (2011), *European Union organised crime threat assessment 2011,*
136. Schloenhardt, A., (1999), Organized crime and the business of migrant trafficking. *Crime, Law and Social Change*, **32**(3): p. 203-233, 10.1023/A:1008340427104.
137. Schloenhardt, A., F. Douglas, and J. Lelliott, (2012), *Stop the planes!? Document fraud and migrant smuggling by air in Australia,* http://www.abc.net.au/am/content/2012/s3465202.htm
138. United Nations Office on Drugs and Crime (UNODC),, (2013), *Transnational Organised Crime in East Asia and the Pacific: A threat assessment,*
139. Australian Criminal Intelligence Commission (ACIC), (2017), Organised Crime in Australia.
140. Kephart, J., (2015), Assuring identity against the growing terrorist travel threat. *Biometric Technology Today*, **2015**(6): p. 5-7, https://doi.org/10.1016/S0969-4765(15)30096-5.
141. Willox, N.A. and T.M. Regan, (2002), *Identity Fraud: Providing a Solution,* Economic Crime Institute and LexisNexis.
142. Europol,, (2009), *European Union organised crime threat assessment 2009, https://www.europol.europa.eu/cms/sites/default/files/documents/octa2009_0.pdf*
143. Moulin, S.L., et al., (2024), Cross-border forensic profiling of fraudulent identity and travel documents: A pilot project between France and Switzerland. *Science & Justice*, **64**(2): p. 202-209, https://doi.org/10.1016/j.scijus.2024.01.003.
144. Baechler, S., (2015), *Des faux documents d'identité au renseignement forensiqu : développement d'une approche systématique et transversale du traitement de la donnée forensique à des fins de renseignement criminel*, (Doctoral), University of Lausanne, Lausanne, Switzerland.
145. Felson, M. and R.V. Clarke, (1998), *Opportunity makes the thief: Practical theory for crime prevention,*
146. Cohen, L.E. and M. Felson, (1979), Social Change and Crime Rate Trends: A Routine Activity Approach. *American sociological review*, **44**(4): p. 588-608, 10.2307/2094589.
147. Reppetto, T., (1976), Crime prevention and the displacement phenomenon. *Crime and Delinquency*, **22**: p. 166-177,
148. Gabor, T., (1981), The crime displacement hypothesis: An empirical examination. *Crime and Delinquency*, **26**: p. 390-404,
149. Hesseling, R., *Displacement: a review of the empirical literature*, in *Crime Prevention Studies*, R.V. Clarke, Editor. 1994, Criminal Justice Press: Monsey, NY. p. 197-230.
150. Ribaux, O., S. Birrer, and S.J. Walsh. *A three level architecture for the analysis of serial burglary that integrates crime mapping tools and forensic case data*. in *European Academy of Forensic Sciences*. 2003. Istanbul, Turkey.
151. Margot, P., *La trace comme vecteur fondamental de la police scientifique*, in *L'expertise en police scientifique*, Y. Ricordel, Editor. 2011: Paris, France.
152. Alooba.com, (2024), *Distance Metrics,* https://www.alooba.com/skills/concepts/statistics/distance-metrics/#:~:text=In%20simpler%20terms%2C%20distance%20metrics,they%20are%20from%20each%20other.
153. Egger, S.A., (1984), A working definition of serial murder and the reduction of linkage blindness. *Journal of Police Science & Administration*, **12**(3): p. 348-357,

154. Camargo, J., et al., (2012), Monitoring of illicit pill distribution networks using an image collection exploration framework. *Forensic Science International*, **223**(1-3): p. 298-305, 10.1016/j.forsciint.2012.10.004.
155. Harris, C. and M. Stephens, (1988), A combined corner and edge detector. *Alvey Vision Conference*, **15**(50),
156. Vieira, R., et al., (2017), *Automatic Documents Counterfeit Classification Using Image Processing and Analysis* [Conference 10.1007/978-3-319-58838-4_44.
157. Vieira, R., et al., (2016), Information System for Automation of Counterfeited Documents Images Correlation. *Procedia Computer Science*, **100**: p. 421-428, 10.1016/j.procs.2016.09.178.
158. Lowe, D.G., (2004), Distinctive image features from scale-invariant keypoints. *International Journal of Computer Vision*, **60**(2): p. 91-110,
159. Ojeda-Aciego, M. and J.M. Rodriguez-Jimenez, (2021), Formal concept analysis with negative attributes for forgery detection. *Computational and mathematical methods*, **3**(6): p. n/a, 10.1002/cmm4.1124.
160. Girelli, C.M.A., (2016), The use of fingerprints available on the web in false identity documents: Analysis from a forensic intelligence perspective. *Forensic Science International (Online)*, **262**: p. 84-96, http://dx.doi.org/10.1016/j.forsciint.2016.02.041.
161. Girelli, C.M.A., (2015), Laterally reversed fingerprints detected in fake documents. *Journal of Forensic Identification*, **65**(1): p. 1-17,
162. Ribaux, O., S. Baechler, and Q. Rossy, *Forensic Intelligence and Traceology in Digitalised Environments: The Detection and Analysis of Crime Patterns to Inform Practice*, in *The Handbook of Security*, M. Gill, Editor. 2022, Palgrave Macmillan, Cham. p. 81-100.
163. Baechler, S., (personal communication, 06/02/2024)
164. Huber, R.A., (1972), The Philosophy of Identification. *RCMP Gazette*, **34**(7 & 8): p. 9-14,
165. Europol, (2020), *France nabs the leaders of a document fraud network active in the EU,* Europol Media & Press, https://www.europol.europa.eu/media-press/newsroom/news/france-nabs-leaders-of-document-fraud-network-active-in-eu
166. Australian Crime Commission (ACC),, (2015), *Organised Crime in Australia 2015, https://www.acic.gov.au/sites/default/files/2016/06/oca2015.pdf?acsf_files_redirect*
167. Smith, R.G., (2018), *Organised Crime Research in Australia 2018,*
168. Voce, I., et al., (2024), *Motives and pathways for joining outlaw motorcycle gangs,*
169. Kirk, P.L., (1963), The Ontogeny of Criminalistics. *Journal of Criminal Law, Criminology & Police Science*, **54**(2): p. 235-238, 10.2307/1141173.
170. Rumbaugh, J., et al., (1991), *Object-oriented Modeling and Design,* Prentice-Hall International.
171. Yang, S., F. Keller, and L. Zheng, (2017), *Social network analysis : methods and examples,* SAGE Publications, Inc.
172. Devlin, C., et al., (2022), The potential of using the forensic profiles of Australian fraudulent identity documents to assist intelligence-led policing. *Australian Journal of Forensic Sciences*, **55**(6): p. 720-730, 10.1080/00450618.2022.2074138.
173. Medina, R.M., (2014), Social Network Analysis: A case study of the Islamist terrorist network. *Security Journal*, **27**(1): p. 97-121, http://dx.doi.org/10.1057/sj.2012.21.

174. Wasserman, S. and K. Faust, (1994), *Social network analysis : methods and applications,* Cambridge University Press.
175. Swiss Federal Office of Police, (2019), *FRAUDE 2017/18: National comparative statistics of fraudulent documents and fraudulent use of documents,* S.F.O.o. Police,
176. Keesing ID Academy, (2018), Study of forgeries: optical variable device, Keesing Technologies.
177. Local Constable, (personal communication, 06/05/2020)
178. McGloin, J.M., (2005), Policy and intervention considerations of a network analysis of street gangs. *Criminology & Public Policy*, **4**(3): p. 607-635, https://doi.org/10.1111/j.1745-9133.2005.00306.x.
179. Sabon, L., S. Yang, and Q. Zhang, (2023), Social Network Analysis of a Latino Sex Trafficking Enterprise. *Journal of Human Trafficking*, **9**(3): p. 263-279, 10.1080/23322705.2021.1898830.
180. Morselli, C., et al., (2009), *Inside Criminal Networks, (1st 2009.),* Springer New York.
181. Bright, D.A. and J.J. Delaney, (2013), Evolution of a drug trafficking network: Mapping changes in network structure and function across time. *Global Crime*, **14**(2-3): p. 238-260, 10.1080/17440572.2013.787927.
182. Morgan, A., et al., *Organised and transnational crime: the impact on Australian police*, in *Australian Policing: Critical Issues in 21st Century Police Practice*, P. Birch, M. Kennedy, and E. Kruger, Editors. 2021, Routledge: Abingdon, Oxford.
183. Morgan A. and Dowling C., (2023), *Enablers of illicit drug trafficking by organised crime groups,*
184. Langhorn, M., (2018), Human trafficking and sexual servitude: Organised crime's involvement in Australia. *Salus Journal*, **6**(1): p. 1-25,
185. Lozusic, R., (2002), *Gangs in NSW,*
186. Global Initiative Against Organized Crime (GI-TOC), (2023), *Global Organized Crime Index - Australia,* Geneva, Switzerland, https://ocindex.net/country/australia
187. Smith, R. and A. Hickman, (2022), *Estimating the costs of serious and organised crime in Australia, 2020-21,*
188. Holmes, L., *Introduction*, in *Terrorism, organised crime and corruption*, L. Holmes, Editor. 2007, Edward Elgar Publishing: Cheltenham. p. 1-28.
189. Corruption and Crime Commission of Western Australia (CCC WA),, (2005), *Report to the joint standing committee on the Corruption and Crime Commission with regard to the Commission's organised crime function and contempt powers, https://www.ccc.wa.gov.au/sites/default/files/Organised%20Crime%20report%20to%20the%20Joint%20Standing%20Committee.pdf*
190. United Nations Office on Drugs and Crime (UNODC),, (2009), *Global report on trafficking in persons,*
191. Parliament of Victoria,, (2010), *Inquiry into people trafficking for sex work,*
192. Morri, M., (2017), Identity theft: Ruthless gangs use fake driver-licences and Medicare cards for crime sprees., *Daily Telegraph*,
193. Statistics, A.B.o., (2022), *Recorded Crime - Offenders 2020-21,* https://www.abs.gov.au/statistics/people/crime-and-justice/recorded-crime-offenders/latest-release#australia
194. Margot, P., (2011), Forensic science on trial - What is the law of the land? *Australian Journal of Forensic Sciences*, **43**(2/3): p. 89-103, 10.1080/00450618.2011.555418.

195. Morelato, M., (2015), *Forensic drug profiling: a tool for intelligence-led policing*, (Doctoral), University of Technology, Sydney, Sydney, Australia.
196. Global Initiative Against Organized Crime (GI-TOC), (2023), *Global Organized Crime Index - Switzerland,* Geneva, Switzerland, https://ocindex.net/country/switzerland
197. INTERPOL, (n.d.), *How INTERPOL supports Australia to tackle international crime,* https://www.interpol.int/en/Who-we-are/Member-countries/Asia-South-Pacific/AUSTRALIA
198. Abrahamson, D.E. and J. Goodman-Delahunty, *Working with others - Future policing partnerships*, in *Australian Policing: Critical Issues in 21st Century Police Practice*, P. Birch, M. Kennedy, and E. Kruger, Editors. 2021, Routledge. p. 199-220.
199. Romagna, M., (2015), Cybermarket for forged identity documents: The illegal trade of identity documents on the surface web and in Onionland. *Keesing Journal of Documents and Identity*, **47**: p. 12-15,
200. Holt, T.J. and J.R. Lee, (2020), A Crime Script Analysis of Counterfeit Identity Document Procurement Online. *Deviant Behavior*: p. 1-18, 10.1080/01639625.2020.1825915.
201. Degeneve, C., J. Longhi, and Q. Rossy, (2022), Analysing the digital transformation of the market for fake documents using a computational linguistic approach. *Forensic Science International: Synergy*, **5**: p. 100287, 10.1016/j.fsisyn.2022.100287.
202. Baravalle, A., M. Sanchez Lopez, and L. Sin Wee. *Mining the Dark Web: Drugs and Fake Ids*. in *IEEE 16th International Conference of Data Mining Workshops (ICDMW)*. 2016. Institute of Electrical and Electronics Engineers (IEEE).
203. Broseus, J., et al., (2016), Studying illicit drug trafficking on Darknet markets: Structure and organisation from a Canadian perspective. *Forensic Science International*, **264**: p. 7-14, 10.1016/j.forsciint.2016.02.045.
204. Kavallieros, D., et al., *Understanding the Dark Web*, in *Dark Web Investigation*, B. Akhgar, et al., Editors. 2021, Springer International Publishing: Cham. p. 3-26.
205. Beckstrom, M. and B. Lund, (2019), *Casting Light on the Dark Web : A Guide for Safe Exploration,* Rowman & Littlefield Publishers, Incorporated.
206. Martin, J., J. Cunliffe, and R. Munksgaard, (2019), *Cryptomarkets: A Research Companion,* Emerald Publishing Limited.
207. Gehl, R.W., (2018), *Weaving the dark web: Legitimacy on Freenet, Tor, and I2P, (1st),* MIT Press.
208. Bedi, P., N. Gupta, and V. Jindal, *Dark Web: A Boon or a Bane*, in *Encyclopedia of Criminal Activities and the Deep Web*, M. Khosrow-Pour D.B.A, Editor. 2020, IGI Global: Hershey, PA, USA. p. 152-164.
209. Collier, B., (2024), *Tor: From the Dark Web to the Future of Privacy,* MIT Press.
210. Jadoon, A.K., et al., (2019), Forensic Analysis of Tor Browser: A Case Study for Privacy and Anonymity on the Web. *Forensic Science International*, **299**: p. 59-73, https://doi.org/10.1016/j.forsciint.2019.03.030.
211. Markoff, J., (2005), *What the Dormouse said: How the sixties counterculture shaped the personal computer industry,* Penguin Books.
212. Zimmerman, P.R., (1999), *Why I wrote PGP,* https://www.philzimmermann.com/EN/essays/WhyIWrotePGP.html
213. Greenberg, A., (2013), An interview with a digital drug lord: The Silk Road's Dread Pirate Roberts (Q & A), *Forbes*,

214. Christin, N. *Traveling the silk road: a measurement analysis of a large anonymous online marketplace*. in *Proceedings of the 22nd international conference on World Wide Web*. 2013. Rio de Janeiro, Brazil: Association for Computing Machinery.
215. Langley, P. and A. Leyshon, (2017), Platform capitalism: The intermediation and capitalisation of digital economic circulation. *Finance and Society*, **3**(1): p. 11-31, 10.2218/finsoc.v3i1.1936.
216. Martin, J., (2014), *Drugs on the dark net: How cryptomarkets are transforming the global trade in illicit drugs (Kindle edition),* Palgrave Macmillan.
217. Aldridge, J. and D. Decary-Hetu, (2014), Not an "eBay for Drugs": The cryptomarket "Silk Road" as a paradigm shifting criminal innovation. *SSRN Electronic Journal*, https://dx.doi.org/10.2139/ssrn.2436643.
218. Soska, K. and N. Christin, (2015), *Measuring the Longitudinal Evolution of the Online Anonymous Marketplace Ecosystem* [Conference paper],Proceedings of the 24th USENIX Security Symposium,
219. Europol, (2021), *Operation Onymous,* https://www.europol.europa.eu/operations-services-and-innovation/operations/operation-onymous
220. Decary-Hetu, D. and L. Giommoni, (2017), Do police crackdowns disrupt drug cryptomarkets? A longitudinal analysis of the effects of Operation Onymous. *Crime Law and Social Change*, **67**(1): p. 55-75, 10.1007/s10611-016-9644-4.
221. Van Buskirk, J., et al., (2017), The recovery of online drug markets following law enforcement and other disruptions. *Drug and Alcohol Dependence*, **173**: p. 159-162, 10.1016/j.drugalcdep.2017.01.004.
222. Dittus, M., J. Wright, and M. Graham. *Platform Criminalism*. in *27th World Wide Web (WWW) Conference*. 2018. Lyon, France: Association for Computing Machinery.
223. Martin, J., et al., (2018), The international darknet drugs trade - a regional analysis of cryptomarkets. *Australasian Policing*, **10**(3): p. 25-29,
224. Caudevilla, F., et al., (2016), Results of an international drug testing service for cryptomarket users. *The International Journal of Drug Policy*, **35**: p. 38-41, 10.1016/j.drugpo.2016.04.017.
225. Van Buskirk, J., et al., (2016), Characterising dark net marketplace purchasers in a sample of regular psychostimulant users. *The International Journal of Drug Policy*, **35**: p. 32, 10.1016/j.drugpo.2016.01.010.
226. Ladegaard, I., (2019), Crime displacement in digital drug markets. *The International Journal of Drug Policy*, **63**: p. 113-121, 10.1016/j.drugpo.2018.09.013.
227. Wood, E., et al., (2004), Displacement of Canada's largest public illicit drug market in response to a police crackdown. *Canadian Medical Association journal (CMAJ)*, **170**(10): p. 1551-1556, 10.1503/cmaj.1031928.
228. Branwen, G., (2019), *Darknet market mortality risks,* https://www.gwern.net/DNM-survival.
229. Goonetilleke, P., A. Knorre, and A. Kuriksha, (2023), Hydra: Lessons from the world's largest darknet market. *Criminology & Public Policy*, **22**(4): p. 735-777, https://doi.org/10.1111/1745-9133.12647.
230. Scott, M.S., (2004), *The Benefits and Consequences of Police Crackdowns,* https://popcenter.asu.edu/content/benefits-and-consequences-police-crackdowns-0

231. Kerr, T., W. Small, and E. Wood, (2005), The public health and social impacts of drug market enforcement: A review of the evidence. *The International Journal of Drug Policy*, **16**(4): p. 210-220, https://doi.org/10.1016/j.drugpo.2005.04.005.
232. Edmunds, M., M. Hough, and N. Urquia, (1996), *Tackling local drug markets,* Great Britain Home Office.
233. Best, D., et al., (2001), Assessment of a Concentrated, High-Profile Police Operation. No Discernible Impact on Drug Availability, Price or Purity. *The British Journal of Criminology*, **41**(4): p. 738-745, 10.1093/bjc/41.4.738.
234. Weatherburn, D.O.N. and B. Lind, (1997), The impact of law enforcement activity on a heroin market. *Addiction (Abingdon, England)*, **92**(5): p. 557-569, 10.1111/j.1360-0443.1997.tb02913.x.
235. Van Buskirk, J., et al., (2014), The closure of the Silk Road: what has this meant for online drug trading? *Addiction*, **109**(4): p. 517-518, https://doi.org/10.1111/add.12422.
236. Ouellet, M., et al., (2022), The Network of Online Stolen Data Markets: How Vendor Flows Connect Digital Marketplaces. *The British Journal of Criminology*, **62**(6): p. 1518-1536, 10.1093/bjc/azab116.
237. Ladegaard, I., (2018), We know where you are, what you are doing and we will catch you : testing deterrence theory in digital drug markets. *The British Journal of Criminology*, **58**(2): p. 414-433, 10.1093/bjc/azx021.
238. Buxton, J. and T. Bingham, (2015), *The Risk and Challenge of Dark Net Drug Markets,* www.drugsandalcohol.ie/23274/1/Darknet%20Markets.pdf.
239. Ladegaard, I., (2020), Open Secrecy: How Police Crackdowns and Creative Problem-Solving Brought Illegal Markets out of the Shadows. *Social forces*, **99**(2): p. 532-559, 10.1093/sf/soz140.
240. Chainalysis Team, *How Darknet Markets and Fraud Shops Fought for Users In the Wake of Hydra's Collapse*. 2023, Chainalysis.
241. Cox, J., (2024), Inside the Underground Site Where 'Neural Networks' Churn Out Fake IDs, *404 Media*,
242. Barratt, M.J. and J. Aldridge, (2016), Everything you always wanted to know about drug cryptomarkets (but were afraid to ask). *The International Journal of Drug Policy*, **35**: p. 1-6, 10.1016/j.drugpo.2016.07.005.
243. Barratt, M.J., et al., (2022), Exploring Televend, an innovative combination of cryptomarket and messaging app technologies for trading prohibited drugs. *Drug and Alcohol Dependence*, **231**: p. 109243-109243, 10.1016/j.drugalcdep.2021.109243.
244. Barratt, M.J., J.A. Ferris, and A.R. Winstock, (2014), Use of Silk Road, the online drug marketplace, in the United Kingdom, Australia and the United States: Silk Road global survey. *Addiction (Abingdon, England)*, **109**(5): p. 774-783, 10.1111/add.12470.
245. Barratt, M.J., J.A. Ferris, and A.R. Winstock, (2016), Safer scoring? Cryptomarkets, social supply and drug market violence. *The International Journal of Drug Policy*, **35**: p. 24-31, 10.1016/j.drugpo.2016.04.019.
246. Broadhurst, R., et al., (2021), *Impact of darknet market seizures on opioid availability,*
247. Morelato, M., et al., (2020), An insight Into Prescription Drugs and Medicine on the AlphaBay Cryptomarket. *Journal of Drug Issues*, **50**(1): p. 15-34, 10.1177/0022042619872955.

248. Chawki, M., (2022), The Dark Web and the future of illicit drug markets. *Journal of Transportation Security*, **15**(3-4): p. 173-191, 10.1007/s12198-022-00252-y.
249. Kruithof, K., et al., (2016), *Internet-facilitated drugs trade: An analysis of the size, scope and the role of the Netherlands,* RAND Corporation.
250. Demant, J., R. Munksgaard, and E. Houborg, (2018), Personal use, social supply or redistribution? Cryptomarket demand on Silk Road 2 and Agora. *Trends in Organized Crime*, **21**(1): p. 42-61, 10.1007/s12117-016-9281-4.
251. Dolliver, D.S., (2015), Evaluating drug trafficking on the Tor Network: Silk Road 2, the sequel. *The International Journal of Drug Policy*, **26**(11): p. 1113-1123, 10.1016/j.drugpo.2015.01.008.
252. Dolliver, D.S., S.P. Ericson, and K.L. Love, (2018), A Geographic Analysis of Drug Trafficking Patterns on the TOR Network. *Geographical Review*, **108**(1): p. 45-68, 10.1111/gere.12241.
253. Jardine, E., (2021), Policing the Cybercrime Script of Darknet Drug Markets: Methods of Effective Law Enforcement Intervention. *American Journal of Criminal Justice*, **46**(6): p. 980-1005, 10.1007/s12103-021-09656-3.
254. Morgenthaler, E. and B. Leclerc, (2023), Crime script analysis of drug importation into Australia facilitated by the dark net. *Global Crime*, **24**(3): p. 169-194, 10.1080/17440572.2023.2212592.
255. Sudan, H.K., et al., (2023), Decrypting the cryptomarkets: Trends over a decade of the Dark Web drug trade. *Drug Science, Policy and Law*, **9**, 10.1177/20503245231215668.
256. Tzanetakis, M., et al., (2016), The transparency paradox. Building trust, resolving disputes and optimising logistics on conventional and online drugs markets. *The International Journal of Drug Policy*, **35**: p. 58-68, https://doi.org/10.1016/j.drugpo.2015.12.010.
257. Holt, T.J. and J.R. Lee, (2023), A crime script model of Dark web Firearms Purchasing. *American Journal of Criminal Justice*, **48**(2): p. 509-529, 10.1007/s12103-022-09675-8.
258. Lee, J.R., T.J. Holt, and O. Smirnova, (2024), An assessment of the state of firearm sales on the Dark Web. *Journal of Crime & Justice*, **47**(1): p. 46-60, 10.1080/0735648X.2022.2058062.
259. Broadhurst, R., et al., (2021), Illicit firearms and other weapons on darknet markets. *Trends and Issues in Crime and Criminal Justice*, (622): p. 1-20,
260. Rhumorbarbe, D., et al., (2018), Characterising the online weapons trafficking on cryptomarkets. *Forensic Science International*, **283**: p. 16-20, 10.1016/j.forsciint.2017.12.008.
261. Holt, T.J., J.R. Lee, and E. O'Dell, (2022), Assessing the Practices of Online Counterfeit Currency Vendors. *Crime & Delinquency*, 10.1177/00111287221134047.
262. Soldner, F., B. Kleinberg, and S.D. Johnson, (2023), Counterfeits on dark markets: a measurement between Jan-2014 and Sep-2015. *Crime Science*, **12**(1): p. 18-19, 10.1186/s40163-023-00195-2.
263. Paul, K.A., (2018), Ancient Artifacts vs. Digital Artifacts: New Tools for Unmasking the Sale of Illicit Antiquities on the Dark Web. *Arts*, **7**(2), 10.3390/arts7020012.
264. Stringham, O.C., et al., (2023), The dark web trades wildlife, but mostly for use as drugs. *People and Nature*, **5**(3): p. 999-1009, 10.1002/pan3.10469.

265. Harrison, J.R., D.L. Roberts, and J. Hernandez-Castro, (2016), Assessing the extent and nature of wildlife trade on the dark web. *Conservation Biology*, **30**(4): p. 900-904, 10.1111/cobi.12707.
266. Roberts, D.L. and J. Hernandez-Castro, (2017), Bycatch and illegal wildlife trade on the dark web. *Oryx*, **51**(3): p. 393-394, 10.1017/S0030605317000679.
267. Roddy, A.L. and T.J. Holt, (2022), An Assessment of Hitmen and Contracted Violence Providers Operating Online. *Deviant Behavior*, **43**(2): p. 139-151, 10.1080/01639625.2020.1787763.
268. Holt, T.J. and J.R. Lee, (2020), A Crime Script Analysis of Counterfeit Identity Document Procurement Online. *Deviant Behavior*: p. 18, 10.1080/01639625.2020.1825915.
269. Romagna, M., (2014), *The cyber-market of identities: criminological analysis on the illegal market of identity documents within the surface Web and Onionland*, (Masters), Utrecht University, Utrecht.
270. DarknetStats, (2020), *Empire Market,* https://www.darknetstats.com/empire-market
271. dnstats, (n.d.), *Empire Market,* https://dnstats.net/site/empire-market/
272. Chatterjee, M., (2021), The demise of White House Market will shake up the Dark Web, *WIRED*, Conde Nast.
273. Cimpanu, C., (2021), Dark web marketplace White House Market shuts down, *The Record*,
274. Munksgaard, R., et al., (2021), Distributing tobacco in the dark: assessing the regional structure and shipping patterns of illicit tobacco in cryptomarkets. *Global crime*, **22**(1): p. 1-21, 10.1080/17440572.2020.1799787.
275. Hout, M.C.V. and T. Bingham, (2013), 'Surfing the Silk Road': A study of users' experiences. *The International Journal of Drug Policy*, **24**(6): p. 524-529, 10.1016/j.drugpo.2013.08.011.
276. Paquet-Clouston, M., D. Décary-Hétu, and C. Morselli, (2018), Assessing market competition and vendors' size and scope on AlphaBay. *The International Journal of Drug Policy*, **54**: p. 87-98, 10.1016/j.drugpo.2018.01.003.
277. Norbutas, L., S. Ruiter, and R. Corten, (2020), Reputation transferability across contexts: Maintaining cooperation among anonymous cryptomarket actors when moving between markets. *The International Journal of Drug Policy*, **76**, 10.1016/j.drugpo.2019.102635.
278. Duxbury, S.W. and D.L. Haynie, (2018), Building them up, breaking them down: Topology, vendor selection patterns, and a digital drug market's robustness to disruption. *Social networks*, **52**: p. 238-250, 10.1016/j.socnet.2017.09.002.
279. van Wegberg, R.S. and T. Verburgh, (2018), *Lost in the Dream? Measuring the Effects of Operation Bayonet on Vendors Migrating to Dream Market'* [Conference paper],Web Science Conference '18,New York, USA, https://doi.org/10.1145/nnnnnnn.nnnnnnn.
280. Baechler, S., et al., (2020), Breaking the barriers between intelligence, investigation and evaluation: a continuous approach to define the contribution and scope of forensic science. *Forensic Science International*, **309**(April 2020), 10.1016/j.forsciint.2020.110213.
281. Spiegel, Y., (2021), The Herfindahl-Hirschman Index and the Distribution of Social Surplus. *Journal of Industrial Economics*, **69**(3): p. 561-594, 10.1111/joie.12253.

282. Eurostat, *Glossary: Herfindahl Hirschman Index (HHI),* https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Glossary:Herfindahl_Hirschman_Index_(HHI)#:~:text=A%20low%20degree%20of%20concentration,whereas%20decreases%20indicate%20the%20opposite.
283. Bellido, L., S. Baechler, and Q. Rossy, (2017), The sale of false identity documents on the internet. *Revue Internationale de Criminologie et de Police Technique et Scientifique*, **70**(2): p. 233-249,
284. Global Drug Survey (GDS), (2018), *Global Drug Survey 2018,* https://www.globaldrugsurvey.com/gds-2018/
285. Global Drug Survey (GDS), (2019), *Global Drug Survey 2019,* https://www.globaldrugsurvey.com/gds-2019/
286. Global Drug Survey (GDS), (2021), *Global Drug Survey 2021,* https://www.globaldrugsurvey.com/gds-2021/
287. Ruey, J., (2018), *La vente de faux documents sur Instagram*, (Masters), University of Lausanne, Lausanne, Switzerland.
288. Federal Bureau of Investigation (FBI),, (2021), *Internet Crime Report 2021, chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf*
289. Wombat Security, (2018), *2018 User Risk Report,*
290. République Française, (2024), *Identity card / Passport: what proof of address?,* https://www.service-public.fr/particuliers/vosdroits/F14807
291. Vedelago, C. and C. Houston, (2016), Fake identities: Buying counterfeit Medicare cards, no questions asked, *The Sydney Morning Herald*,
292. Connolly, K., et al., (2023), Dark Web Marketplaces: Data for Collaborative Threat Intelligence. *Digital Threats*, **4**(4): p. Article 49, 10.1145/3615666.
293. Power, M., (2020), Online Drug Market Empire Disappears, with $30 Million of Users' Money, *Vice News*, Vice.
294. Barrett, B., (2020), *179 Arrested in Massive Global Darkweb Takedown,* https://www.wired.com/story/operation-disruptor-179-arrested-global-dark-web-takedown/
295. Ferrett, L., (2023), *Tor2(run out the back)door: Exit scam or seizure?,* Searchlight. Cyber, https://www.slcyber.io/tor2run-out-the-backdoor-exit-scam-or-seizure/
296. Searchlight Cyber, (n.d.), *Dread,* Searchlight Cyber, https://www.slcyber.io/dark-web/dread/?_gl=1*1mny4k8*_up*MQ..*_ga*NjY2NjkyMjk5LjE3MjA0OTkxNTQ.*_ga_L2EH29MHLE*MTcyMDQ5OTE1NC4xLjAuMTcyMDQ5OTE1NC4wLjAuMA..
297. Document examiner, (personal communication, 03/05/2022)
298. (2018), *Strategic intelligence assessment: Dark net tradecraft after Operation Bayonet,*
299. Office of the Australian Information Commissioner (OAIC), (2018), *Notifiable Data Breaches Statistics Report: 1 January to 31 March 2018,* https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-publications/notifiable-data-breaches-statistics-report-1-january-to-31-march-2018
300. Office of the Australian Information Commissioner (OAIC), (2018), *Notifiable Data Breaches Statistics Report: 1 April to 30 June 2018,*

https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-publications/notifiable-data-breaches-statistics-report-1-april-to-30-june-2018
301. Office of the Australian Information Commissioner (OAIC), (2019), *Notifiable Data Breaches Statistics Report: 1 October to 31 December 2018,* https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-publications/notifiable-data-breaches-statistics-report-1-october-to-31-december-2018
302. Office of the Australian Information Commisioner (OAIC), (2020), *Notifiable Data Breaches Report: January - June 2020,* https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-publications/notifiable-data-breaches-report-januaryjune-2020#:~:text=There%20was%20a%203%25%20decrease,from%20July%20to%20December%202019.&text=Key%20findings%20for%20the%20January,were%20notified%20under%20the%20scheme.
303. Australian Bureau of Statistics (ABS), (2023), *Personal Fraud 2021-2022 Financial Year* [Press Release], Australian Bureau of Statistics (ABS), https://www.abs.gov.au/statistics/people/crime-and-justice/personal-fraud/latest-release
304. Büsgen, A., et al., *From Cracked Accounts to Fake IDs: User Profiling on German Telegram Black Market Channels*. 2023, Springer: Switzerland. p. 176-202.
305. Australian Federal Police (AFP), (2014), Identity unknown?, *AFP Platypus Magazine*, Australian Federal Police.
306. The Commonwealth of Australia,, (2023), *National Strategy for Identity Resilience, https://www.homeaffairs.gov.au/criminal-justice/files/national-strategy-for-identity-resilience.pdf*
307. Branwen, G., (2015), *Tor black-market-related arrests,* https://gwern.net/dnm-arrest
308. Moses, A., (2013), Fake ID sites under investigation, *The Sydney Morning Herald*, Fairfax Media.
309. Cox, J., (2024), 'Neural Network' Fake ID Site Goes Dark After 404 Media Investigation, *404 Media*, 404 Media.
310. Chang, W., (2024), AI Is The Final Blow For An ID System Whose Time Has Passed, *Forbes Innovation*, Forbes Media.
311. Coghlan, J., (2024), *AI-generated fake IDs claimed to pass crypto exchange KYC are selling for $15,* https://cointelegraph.com/news/agribusiness-adopts-esg-practices-to-meet-growing-global-market-demands
312. Victorian Police, (2024), *Online identity theft,* https://www.police.vic.gov.au/online-identity-theft
313. Australian Federal Police (AFP), (2024), *Identity crime,* https://www.afp.gov.au/crimes/fraud-and-corruption/identity-crime-australia
314. New South Wales Police Force (NSWPF), (n.d.), *Identity Theft,* https://www.police.nsw.gov.au/crime/frauds_and_scams/fraud_categories/identity_theft
315. Office of the Australian Information Commissioner (OAIC), (n.d.), *Identity fraud,* https://www.oaic.gov.au/privacy/your-privacy-rights/data-breaches/Identity-fraud
316. Prenzler, T. and R. Sarre, *Community safety, crime prevention, and 21st century policing*, in *Australian Policing: Critical Issues in 21st Century Police Practice*, P. Birch, M. Kennedy, and E. Kruger, Editors. 2021, Routledge: Abingdon, Oxford. p. 283-298.

317. Ransley, J. and L. Mazerolle, (2009), Policing in an era of uncertainty. *Police Practice and Research*, **10**(4): p. 365-381, 10.1080/15614260802586335.
318. Kaldas, N., *Terrorism and the role of state police*, in *Australian Policing: Critical Issues in 21st Century Police Practice*, P. Birch, M. Kennedy, and E. Kruger, Editors. 2021, Routledge: Abingdon, Oxford.
319. Weyermann, C., M. Jendly, and Q. Rossy, (2018), Special Edition on Policing (at) the ESC - Perspectives from the Lausanne School of Criminal Justice: Combining Forensic Science and Criminology to Foster Innovation in Policing. *Policing: A Journal of Policy and Practice*, **13**(1): p. 1-4, 10.1093/police/pay002.
320. Petersilia, J., (1991), Policy Relevance and the Future of Criminology - The American Society of Criminology - 1990 Presidential Address Comments. *Criminology*, **29**(1): p. 1-16,
321. Petersilia, J., (2008), Influencing public policy: An embedded criminologist reflects on California prison reform : tdemy of Experimental Criminology 2007 Joan McCord Prize Lecture. *Journal of Experimental Criminology*, **4**(4): p. 335-356, 10.1007/s11292-008-9060-6.
322. Deckert, A. and R. Sarre, (2017), *The Palgrave Handbook of Australian and New Zealand Criminology, Crime and Justice, (First),* Springer International Publishing AG.
323. Wilson, J.Q. and J. Petersilia, *Introduction*, in *Crime and Public Policy*, J.Q. Wilson and J. Petersilia, Editors. 2011, Oxford University Press: U.S.A.
324. Commonwealth Transnational Serious and Organised Crime Centre (TSOCC), (2018), *National strategy to fight transnational, serious and organised crime,* https://www.homeaffairs.gov.au/nat-security/files/strategy-transnational-serious-organised-crime.pdf
325. Barker, C., *Transnational, serious and organised crime*, in *Parliamentary Library Briefing Book: Key issues for the 46th Parliament*. 2019, Parliament of Australia,: Canberra, ACT.
326. Brown, R. and S. Gillespie, (2015), Overseas financial investigation of organised crime: Examining the barriers to effective implementation. *Journal of money laundering control*, **18**(3): p. 371-381, 10.1108/JMLC-03-2014-0010.
327. Australian Government,, (2009), *Trafficking in Persons: The Australian Government Response January 2004-April 2009,*
328. Attorney General's Department,, (2010), *Trafficking in persons: The Australian Government response,*
329. Australian Federal Police (AFP), (2024), *Serious and organised crime,* Canberra, https://www.afp.gov.au/crimes/serious-and-organised-crime#:~:text=Join%20us-,About%20this%20crime,economic%20prosperity%20and%20social%20harmony.
330. Goodin, D., (2022), "Tough to forge" digital driver's licence is...easy to forge, *Ars Technica*, Conde Nast.
331. Rhumorbarbe, D., et al., (2016), Buying drugs on a Darknet market: a better deal? Studying the online illicit drug market through the analysis of digital, physical and chemical data. *Forensic Science International*, **267**: p. 173-182, 10.1016/j.forsciint.2016.08.032.

Appendix

Appendix

Appendix

The following section includes figures and tables that provide extra information adjacent to the points discussed in this thesis. The following tables and figures are included in this section.

Figures

Tables

Table A. 1: Quick reference outline of the Australian identity crime or related statutes and the different aspects of identity crime that they include

		Identity crime				
State	**Statute/provisions**	Production and manipulation	Acquisition	Possession	Transfer/Trafficking	Use
NSW	Crimes Act 1900 Crimes Amendment (Fraud, Identity and Forgery Offences) Act 2009 No 99 Part 4AB Identity offences	Y	N	Y	Y	Y
NT	Criminal Code Amendment (Identity Crime) Act 2014	Y	N	Y	Y	Y
QLD	Criminal code act 1899 (Qld), amended by the Criminal Code and Civil Liability Amendment Act 2007 (Qld) to include section 408D, "Obtaining or dealing with identification information"	N	Y	Y	Y	Y
SA	Criminal Law Consolidation Act 1935 (SA) Part 5A "Identity theft"	Y	Y	Y (EQUIPMENT)	Y	Y
TAS	Computer fraud Criminal Code Act 1924 Sections 257A to 257E titled "Crimes related to computers". It is a very broad statute Forgery and Uttering	Y	Y	N	Y	Y

	Criminal Code Act 1924 Sections 278, 279 and 285					
VIC	Division 2AA of the Crimes Act 1958 (Vic) Sections 192A-192E	Y	N	Y	Y	Y
WA	Criminal code amendment (identity crime) Act 2010	Y	N	Y	Y	Y

Table A. 2: Identity crime and related statutes used across Australian states, their wording and what portion of identity crime they address

State	Statute/provisions	Identity crime	Wording
NSW	Crimes Act 1900 Crimes Amendment (Fraud, Identity and Forgery Offences) Act 2009 No 99 Part 4AB Identity offences	Production and manipulation	**NSWCA 192J -** Person who deals in identity information (deals = make, use, supply) with intention of committing indictable offence is guilty of an offence
		Acquisition	Not specified
		Possession	**NSWCA 192K and 192L** Person who possesses identification information with intent to commit or to facilitate an indictable offence, possession of any equipment etc. capable of making document or other thing that contains identification information, with the intent to use the document to commit an indictable offence
		Transfer/trafficking	**NSWCA 192J -** Person who deals in identity information (deals = make, use, supply) with intention of committing indictable offence is guilty of an offence
		Use	**NSWCA 192J -** Person who deals in identity information (deals = make, use, supply) with intention of committing indictable offence is guilty of an offence
NT	Criminal Code Amendment (Identity Crime) Act 2014	Production and manipulation	**NTCCA 228C** Dealing in (make, copy, store, supply, transmit or use) identification information with intent
		Acquisition	Not specified
		Possession	**NTCCA 228D & 228E** Possession of identification information with intent, possessing equipment used to deal in identification information or identification documentation

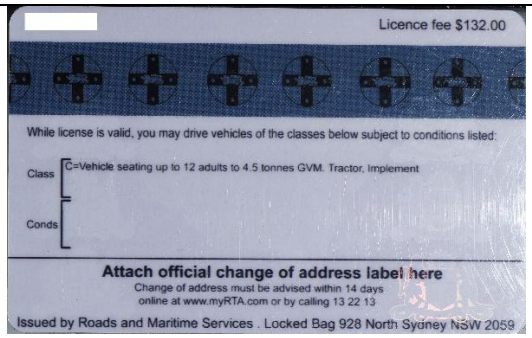
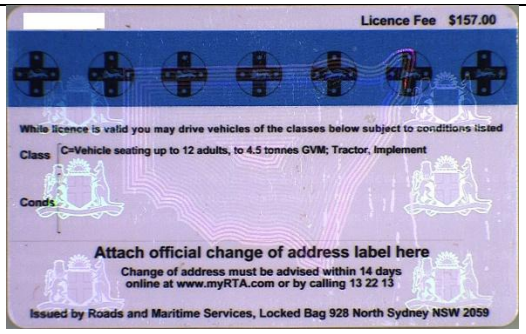
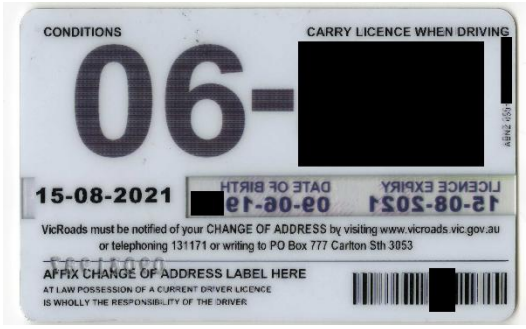
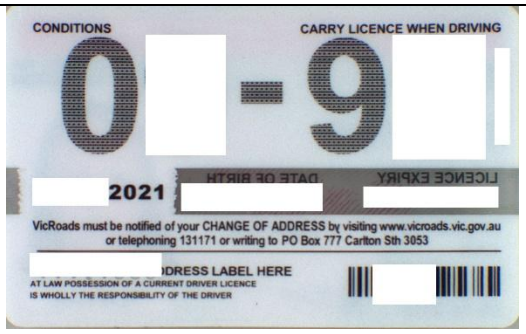
			NTCCA 228C Dealing in (make, copy, store, supply, transmit or use) identification information with intent
		Transfer/trafficking	**NTCCA 228C** Dealing in (make, copy, store, supply, transmit or use) identification information with intent
		Use	**NTCCA 228C** Dealing in (make, copy, store, supply, transmit or use) identification information with intent
QLD	Criminal code act 1899 (Qld), amended by the Criminal Code and Civil Liability Amendment Act 2007 (Qld) to include section 408D, "Obtaining or dealing with identification information"	Production and manipulation	Not specified
		Acquisition	**QCCA 408D (1)** Obtaining identity information for commission of an indictable offence
		Possession	**QCCA 408D (1A)** Possessing equipment to commit an indictable offence involving acquisition, transfer, or use of identity information
		Transfer/trafficking	**QCCA 408D (1)** Dealing with identity information, for commission of indictable offence
		Use	**QCCA 408D (1)** Dealing with identity information, for commission of indictable offence
SA	Criminal Law Consolidation Act 1935 (SA) Part 5A "Identity theft"	Production and manipulation	**SACLCA 144D** Producing prohibited material (anything that enables a person to assume a false identity)
		Acquisition	**SACLCA 144B** Assuming a false identity with intent to commit serious criminal offence
		Possession	**SACLCA 144B** Possessing equipment to make prohibited material
		Transfer/trafficking	**SACLCA 144D** Selling or giving away prohibited material (anything that enables a person to assume a false identity
		Use	**SACLCA 144C** Misuse of person identification

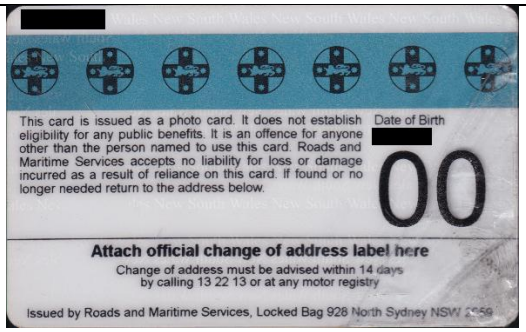
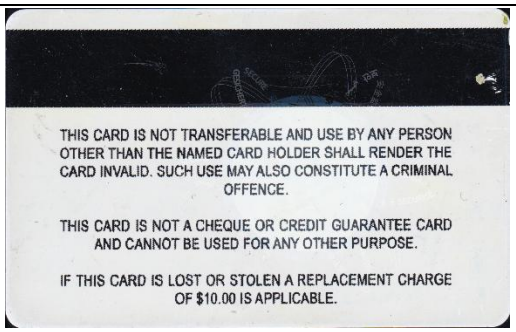
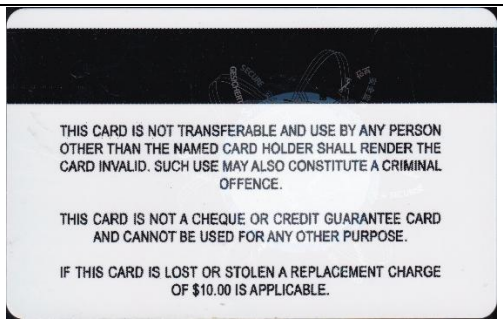
			information, for commission of serious criminal offence
TAS	Computer fraud statute Criminal Code Act 1924 Sections 257A to 257E titled "Crimes related to computers". It is a very broad statute Criminal Code Act 1924 Sections 278, 279 and 285 "Forgery and Uttering*"	Production and manipulation	**TASCCA 257B** A person who, with intent to defraud: 1) destroys, damages, erases, alters or otherwise manipulates data stored in, or used in connection with, a computer; or 2) introduces into, or records or stores in, a computer or system of computers by any means data for the purpose of – a) destroying, damaging, erasing or altering other data stored in that computer or that system of computers; or b) interfering with, interrupting or obstructing the lawful use of that computer or that system of computers or the data stored in that computer or system of computers; or 3) otherwise uses a computer is guilty of a crime **TASCCA 278** Any person who forges any document, seal, or die, with intent to defraud, is guilty of a crime
		Acquisition	**TASCCA 280** Any person who, with intent to defraud, demands, receives, or obtains or procures to be delivered, paid, or transferred to any person any property whatever upon or by virtue of – (a) any forged document whatsoever, knowing it to be forged.
		Possession	Not specified

		Transfer/trafficking	**TASCCA 278** Any person who utters any forged document, seal, or die, is guilty of a crime.
		Use	**TASCCA 278** Any person who utters any forged document, seal, or die, is guilty of a crime.
VIC	Division 2AA of the Crimes Act 1958 (Vic) Sections 192A-192E	Production and manipulation	**VICCA 192B** - it is an offence to make, use, or supply identification information
		Acquisition	Not specified
		Possession	**VICCA 192C & 192D-** it is an offence to possess identification information and equipment to produce identification information
		Transfer/trafficking	**VICCA 192B** - it is an offence to make, use, or supply identification information
		Use	**VICCA 192B** - it is an offence to make, use, or supply identification information
WA	Criminal code amendment (identity crime) Act 2010	Production and manipulation	**WACCA 490** It is an offence to make, use, or supply identification information with intent to commit or facilitate indictable offence
		Acquisition	Not specified
		Possession	**WACCA 491** Possession of identification material with intent to commit indictable offence. Possession of identification equipment (anything used to make, use, supply or retain identification material) with intent
		Transfer/trafficking	**WACCA 490** It is an offence to make, use, or supply identification information with intent to commit or facilitate indictable offence
		Use	**WACCA 490** It is an offence to make, use, or supply identification information with intent to commit or facilitate indictable offence

* **to utter** means to use, offer, publish, deliver, dispose of, tender in payment or in exchange, expose for sale or exchange, exchange, tender in evidence or put off any forged document, seal, or die, with intent to defraud, knowing the same to be forged wheresoever the same may have been forged **TASCCA 1924 Section 277**

Table A. 3: Examples of each of the Australian document types examined and profiled within this research. Redacted examples of the front and back of each document have been provided. International licences have not been included.

Document Type	Front	Back
Counterfeit NSW Drivers Licence (Unrestricted)		
Counterfeit NSW Drivers Licence (Provisional)		
Counterfeit VIC Drivers Licence (Unrestricted)		
Counterfeit VIC Drivers Licence (Provisional)		

Counterfeit WA Drivers Licence (Unrestricted)		
Counterfeit WA Drivers Licence (Provisional)		
Forged NSW Photo card		
Pseudo NSW Student identification		
Pseudo NSW Age proof card		

(a)

(b)

Figure A. 1: Image of scanned document with background canvas. The entire canvas is an A4 sheet of thick, satin paper, this is cropped to just show the main features of interest, along with where the document and QR codes should be located on the canvas. The two QR codes above the document are the QR codes generated by BIDIF when uploading the documents. Image (a) is an example of the front of the document (recto), and (b) is an example of the back (verso).

Table A. 4: The intrinsic and extrinsic decision criteria for feature selection within the profiling method from Baechler et al. 2015 [14].

	Criteria	Explanation
Intrinsic criteria (relative to the features themselves and their origin)	Low intra-variability	No or low amount of variation within a group of traces from the same source
	High inter-variability	Significant variation among traces of different sources
	Complementarity	The features must be as independent as possible
	Representativeness	Reflects the features/characteristics of the source(s)/activity(ies) used to create the document
	Comparability	The features of the trace must be comparable to the features of the other traces to ensure that they can be compared regarding their similarity/differences
	Availability and completeness	The feature must be constantly and completely measurable within the population of interest
Extrinsic criteria (related to the observation and measurement methods)	Non-destructiveness	Does not alter or destroy the trace
	Sensitivity	Returns a positive result when the feature is present
	Specificity	Returns a negative result when the feature is absent
	Reproducibility and reliability	Consistency of results when feature extraction is conducted by different operators, or different equipment at different times or locations
	Low resource requirement	Low requirements for time, cost, equipment, knowledge, and training
	Accessibility	Equipment and knowledge required to extract/ identify the feature are readily available, and the trace is readily available to extract with the correct equipment and knowledge

	Adaptability	Ability to follow up on the evolution and mutations of the feature

Table A. 5: Examples of characteristics of interest used in the profile for each NSW counterfeit licence examined. Features of the same type have been grouped for ease. Features that are made up of several characteristics have been highlighted in the image of the feature rather than outlining each individual feature (e.g. the state badge and the UV coat of arms). Note: COA = Coat of arms, and OVD = Optically variable device. This is not an exhaustive list of all features examined.

For confidentiality reasons this table has been removed from this copy of the document. If you wish to view the table, please reach out to the author.

Table A. 6: Examples of characteristics of interest used in the profile for each WA counterfeit licence examined. Features of the same type have been grouped for ease. Features that are made up of several characteristics have been highlighted in the image of the feature rather than outlining each individual feature (e.g. the state badge and the UV coat of arms). Note: COA = Coat of arms, and OVD = Optically variable device. This is not an exhaustive list of all features examined.

For confidentiality reasons this table has been removed from this copy of the document. If you wish to view the table, please reach out to the author.

Table A. 7: Examples of characteristics of interest used in the profile for each VIC counterfeit licence examined. Features of the same type have been grouped for ease. Features that are made up of several characteristics have been highlighted in the image of the feature rather than outlining each individual feature (e.g. the state badge and the UV coat of arms). Note: COA = Coat of arms, and OVD = Optically variable device. This is not an exhaustive list of all features examined.

For confidentiality reasons this table has been removed from this copy of the document. If you wish to view the table, please reach out to the author.

Figure A. 2: Padif analysis 2 ROIs for the NSW counterfeit licences, the front of the document on the left, and the back on the right

Figure A. 3: Padif analysis 3 ROIs for the NSW counterfeit licences, the front of the document on the left, and the back on the right

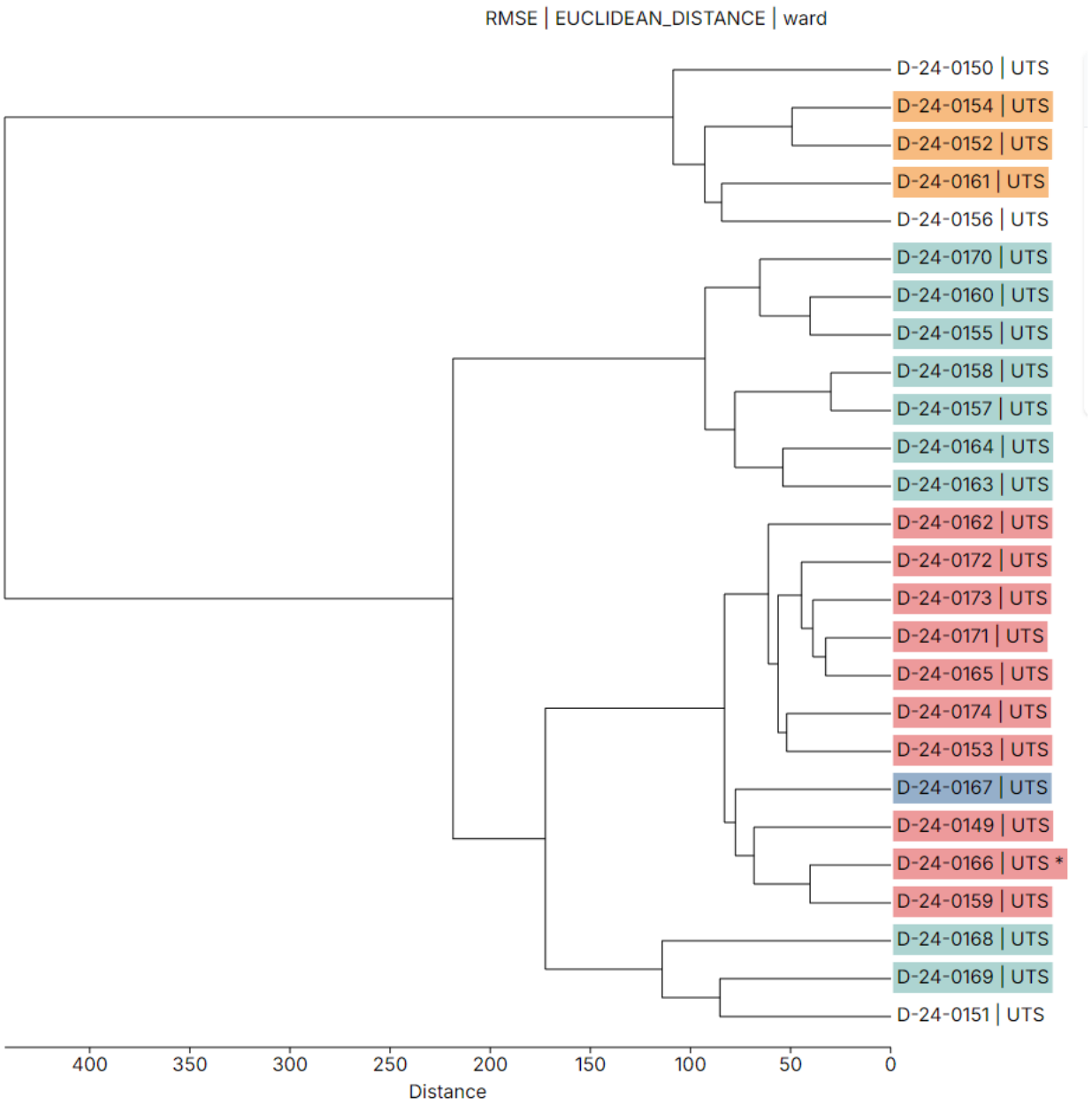


Figure A. 4: The dendrogram results from Padif analysis 2. Each colour designates the series that the document was identified as belonging to based on the manual profiling (NSW_DL1 = pale teal, NSW_DL2 = red, NSW_DL3 = orange, NSW_DL5 = blue).

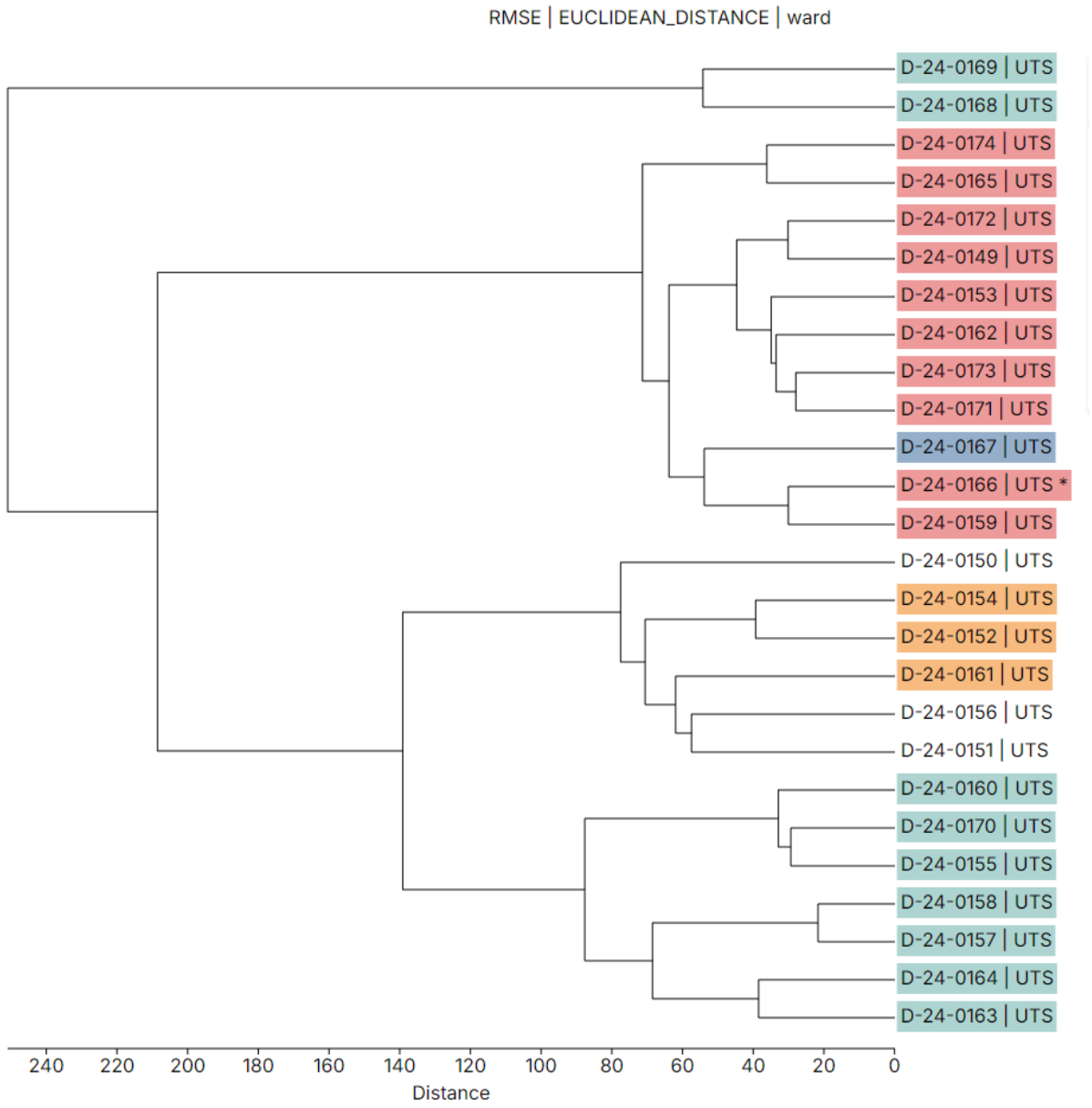


Figure A. 5: The dendrogram results from Padif analysis 3. Each colour designates the series that the document was identified as belonging to based on the manual profiling (NSW_DL1 = pale teal, NSW_DL2 = red, NSW_DL3 = orange, NSW_DL5 = blue).

Table A. 8: Different dark web internet networks

Network	Explanation
Freenet	This dark web network was originally created to promote censorship resistant communication and anonymous publishing by protecting the identities of the uploader of the content and the person retrieving the information [205]. It uses a distributed file storage system, so when information is inserted into a Freenet site it is broken down and distributed to different servers on the internet. Much like a pirate distributing their treasure across multiple hiding places. When an individual then accesses that content, or a piece of it, it is retrieved from the different servers and put back together [205]. While Tor and Freenet are different in their functionality and mechanics, they both essentially create tunnels or niches within the existing internet to house their content. This means that the regular internet still exists around the two networks, and in Tor regular internet content is still accessible (i.e. the deep and surface web content). However, the hidden content on the dark web cannot easily be stumbled upon, the user must know where it is and have the tools to access it. For example, the .onion addresses consist of sixteen alphanumeric characters, so in order to successfully navigate to an .onion site, the user must know where they are intending to go [204].
The Invisible Internet Project (i2P)	While Tor and Freenet exist within the regular internet structure as tunnels or niches, i2P is essentially a network that sits on top of the internet, keeping the traditional internet separate from it. Similarly to Tor it keeps the movements and identities of the users private by utilising nodes to disguise the individual's traffic [205]. However, where Tor creates layers, the idea behind i2P is to overload the traffic with 'pings' like the way cell towers pick up movements based on the cell tower that a device 'pings' off. By creating so many pings at the same time, no outside observer can identify where the user is originating from [205].
Friend to friend (F2F) and Peer to	These are smaller, simple connections between two or more computers on the internation to share information [205].

peer (P2P) networks

Table A. 9: Definitions of product categories from the overall market used to organise the listings from WHM and Empire Market

Product Category	Definition
Illicit drugs	Contains all listings for illicit drugs, what has been considered as illicit are all drugs that are deemed as illegal within Australia, i.e. those where the most common use is illicit
Prescription drugs and medicines	All products that can be purchased from a pharmacy (with or without a prescription)
Custom/other	Any listings that have been specifically created for an individual buyer, along with other miscellaneous items such as shipping charges and tip jars. Most often these listings will not contain any product-specific information but will rather have a title that specifies the buyer that the order is for, such as "custom order for chxxxxx23".
Fraud related	Contains the broadest range of products across these marketplaces, including information dumps, money laundering services, cracked accounts (such as Netflix, pornography subscriptions and software), malware, and other cybercrime-related items and others. The 'fraud related' category has been used to group all listings that are related to fraudulent activities, except for identity fraud.
Goods, currencies and precious metals	This category groups all listings for counterfeit goods such as clothing and accessories, counterfeit currencies, bitcoin related products, and any precious metals like gold.
ID-related	Covers all listings that are related to personal information and other information required to facilitate identity crime, as well as identity documents.
Guides and tutorials	All listings that contained guidebooks, how-tos, recipes and the like. This category includes a range of guides, from 'how to be an alpha male', to exercise videos, recipes for the manufacture of illicit drugs, lock picking, and how to commit a range of cybercrime and fraud activities among others.
Performance and image enhancing drugs (PIEDs)	This category includes all listings for drugs that can be used to increase the performance or physical attributes of an individual, including body augmentation drugs. This includes things such as steroids, diet pills and Botox.
Lab supplies & paraphernalia	This category includes all things that are used in the manufacture of illicit drugs and chemicals, includes things such as drug pre-cursors, glassware, and paraphernalia used to facilitate drug use such as bongs, syringes, spoons and packaging for drugs.
Weapons	Includes all items that can be considered weapons, such as firearms, ammunition, knives, tasers, pepper spray etc.

Table A. 10: Average, median, minimum and maximum prices for all product categories across the ID-Related market, for both physical and digital products. In most cases physical products are more expensive than the digital products, with some exceptions. The most expensive digital products, as indicated by the maximum prices, were for 100 selfie ID's ($3,333), a registered IELTS certificate ($1,885), and what is listed as a copy of the barcode generation software used by the DMV, the government body that generates licences in the US ($1,393). The greyed-out cells indicate that there were no products of that type listed in that category.

			Price (AUD)			
			Average	**Median**	**Minimum**	**Maximum**
ID	Passport	Physical	$9,641	$2,713	$14	$56,828
		Digital	$32	$21	$1	$139
	ID pack	Physical	$7,881	$3,623	$29	$22,615
		Digital	$112	$72	$1	$497
	Licence	Physical	$578	$258	$21	$5,827
		Digital	$31	$14	$1	$923
	ID various	Physical	$863	$716	$15	$4,972
		Digital	$78	$32	$1	$665
	Identity card	Physical	$698	$327	$105	$5,608
		Digital	$29	$14	$4	$251
	Other	Physical	$121	$33	$2	$46
		Digital	$36	$32	$4	$1,393
	Selfie ID bulk	Physical	-	-	-	-
		Digital	$1,582	$989	$325	$3,334
Identity fraud	Fullz	Physical	-	-	-	-
		Digital	$55	$16	$0.15	$2,344
	Identity fraud pack	Physical	-	-	-	-
		Digital	$48	$7	$0.70	$592
	Other	Physical	-	-	-	-
		Digital	$28	$14	$8	$63
Various legitimation documents	Other	Physical	$598	$213	$1	$2,897
		Digital	$66	$35	$1	$1,885
	Statements	Physical	$71	$71	$45	$98
		Digital	$25	$7	$1	$142

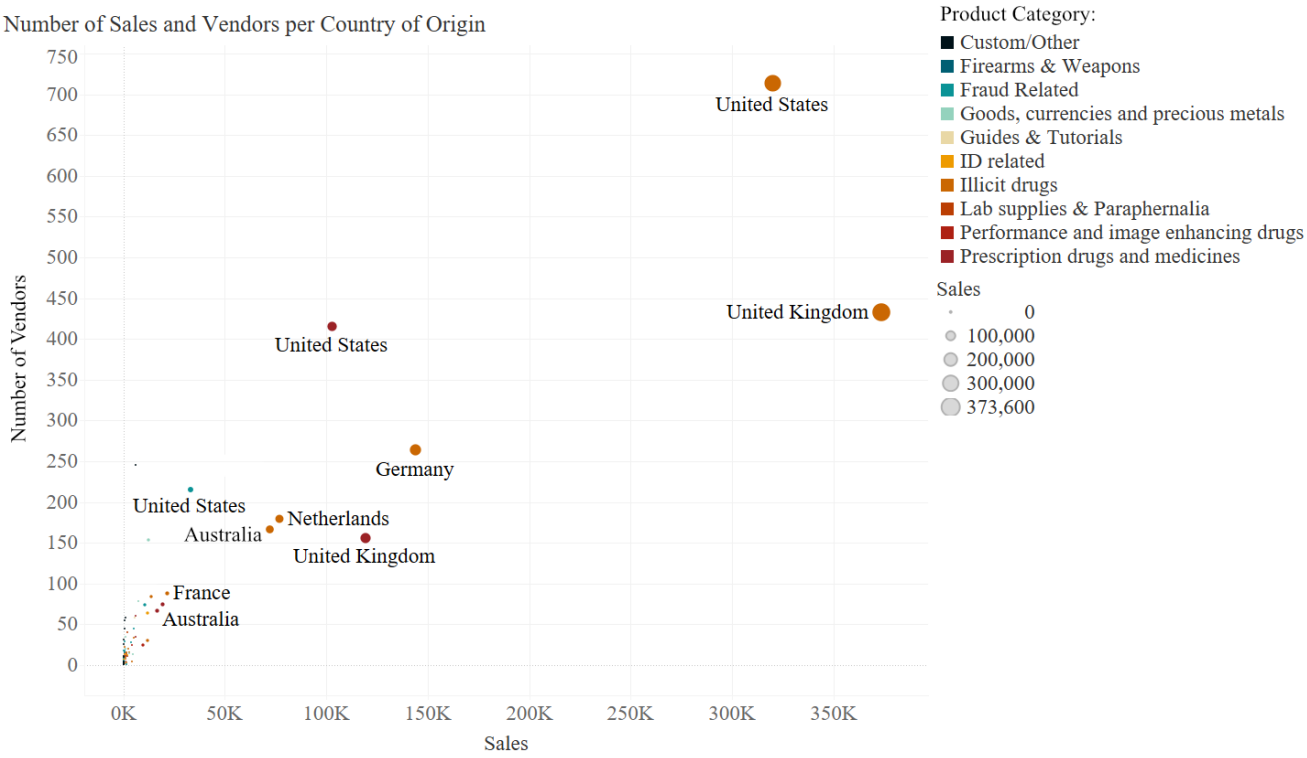


Figure A. 6: Number of sales and vendors per origin country on Empire. The colour indicates the product category that the sales are coming from, with the size indicating the number of sales

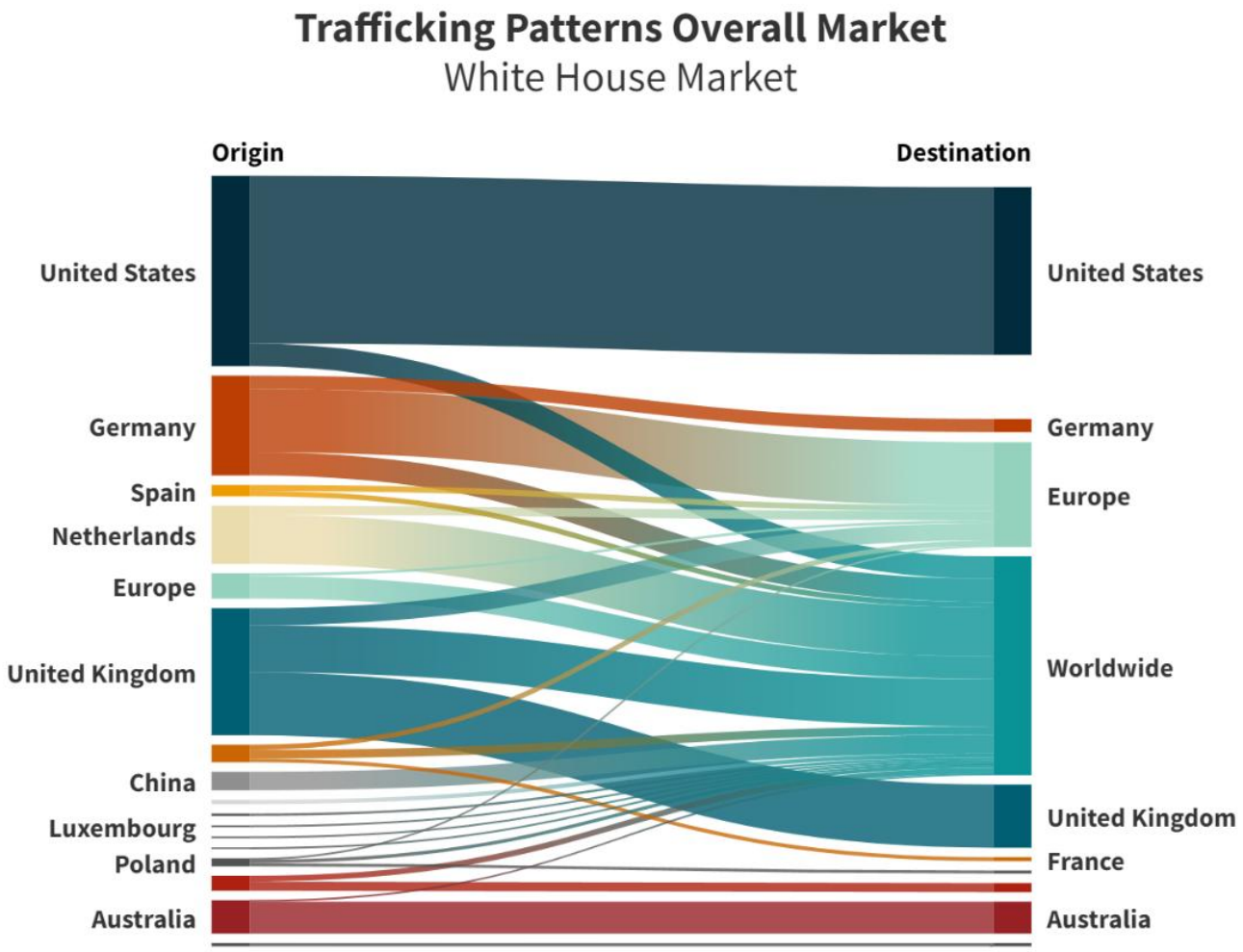


Figure A. 7: Sankey-Alluvial diagram illustrating the movement of goods from origin to destination countries on WHM. This is based off product listings, and only those origin: destination combinations with greater than 0.2% frequency have been included

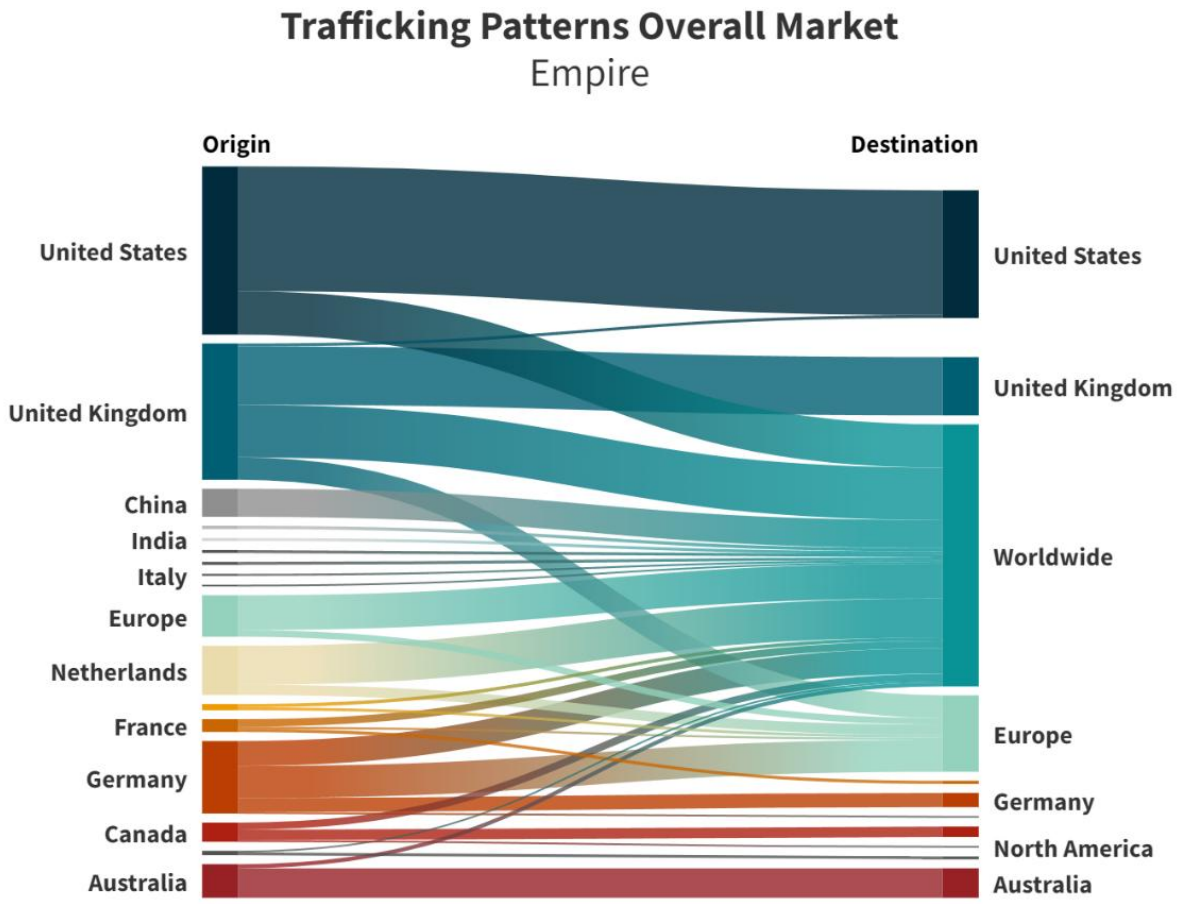


Figure A. 8: Sankey-Alluvial diagram illustrating the movement of goods from origin to destination countries on Empire. This is based off product listings, and only those origin: destination combinations with greater than 0.2% frequency have been included