Forensic Science International 363 (2024) 112203

Contents lists available at ScienceDirect

Forensic Science International

journal homepage: www.elsevier.com/locate/forsciint

Illuminating the dark web market of fraudulent identity documents and personal information: An international and Australian perspective

Ciara Devlin [a,*], Scott Chadwick [a], Sébastien Moret [a,b], Simon Baechler [c,d,e], Quentin Rossy [d], Marie Morelato [a]

[a] University of Technology Sydney, Centre for Forensic Science, PO Box 123, Broadway, NSW 2007, Australia
[b] University of Derby, School of Human Sciences, College of Science and Engineering, Kedleston Rd, Derby DE22 1GB, United Kingdom
[c] Groupe de Recherche en Science Forensique, Université du Québec à Trois-Rivières, Canada
[d] Ecole des Sciences Criminelles, University of Lausanne, Lausanne, Switzerland
[e] Department of Forensic Science and Crime Intelligence, Police Neuchâteloise, Switzerland

ARTICLE INFO

Keywords:
Forensic intelligence
Cryptomarkets
Fraudulent identity documents
Anonymous online marketplaces
Dark web

ABSTRACT

From the beginnings of Silk Road in 2011, anonymous online marketplaces have continued to grow despite the best efforts of law enforcement. While these ever-present marketplaces remain flooded with illicit drugs and related paraphernalia, the sale and distribution of fraudulent identity documents remains a persistent problem, with these items consistently appearing for sale on both the open and dark web. While fraudulent Australian documents are some of the most popular products for sale, there is still much that is unknown about the Australian criminal market and its place within anonymous online marketplaces. Given the success of previous research in understanding the illicit drug trade through examining these marketplaces, this work examines two markets to gain an understanding of where Australian document fraud sits within this digital ecosystem. Two anonymous online marketplaces were crawled across 2020 and 2021, White House Market (WHM), and Empire Market. This data was extracted and examined to identify trends within both the international online market and the online market specifically for Australian documents, both of which have been relatively underexplored in the online space. To help illuminate the features of the market, the types of documents for sale, supply and demand trends, and trafficking flows along with vendor-related trends (e.g. product diversification and presence across markets) were examined. Each market was examined individually and then, where possible, comparisons were drawn to gain a more holistic understanding of the online fraudulent document market, with a specific focus on Australian products. Results indicate that, while the fraudulent document portion of the market is small, it is diverse, with numerous different identity-related products for sale, the most common being driver's licences from the United States (U.S.) and Australia, with digital documents dominating the whole marketplace. Overall, the most popular U.S. products were those that could be used to facilitate identity fraud, with the most popular Australian products being driver's licences and ID packs, likely linked to the presence of the 100-point identity check system used in Australia. This study demonstrates that anonymous online marketplaces have thus far been under-utilised in the study of the fraudulent document market, and that to properly understand the illicit market for fraudulent documents and personal information both the online and physical sides of the market should be considered. This information, if properly utilised, can improve the current understanding of this persistent criminal environment, building on previous research and assisting policymakers in making informed decisions.

1. Introduction

The ability for an individual to legally exist in society is greatly enabled by that person's capacity to prove their identity, most often through a range of identity documents such as driver's licences, passports, and identity cards. It has become globally recognised that these sorts of identity documents are pivotal aspects of social, political, and economic life [1,2], as they provide individuals access to travel, employment, and health care along with a range of other governmental benefits. The advantage of possessing a secure legal identity is clear, and

* Corresponding author at: 15 Broadway, Ultimo, NSW 2007, Australia.
E-mail address: Ciara.j.devlin@student.uts.edu.au (C. Devlin).

https://doi.org/10.1016/j.forsciint.2024.112203
Received 28 February 2024; Received in revised form 4 August 2024; Accepted 20 August 2024
Available online 22 August 2024

criminals have long understood the value of identity documents with them being an item of interest since their implementation [1]. The ability to travel across borders with ease in combination with the ability to remain anonymous has resulted in identity documents, and most notably fraudulent identity documents, becoming a facilitator and enabler for criminal activities including the trafficking of illicit goods, migrant smuggling, organised crime, and terrorism [1,3–8]

Due to their high value, a strong, international online market for stolen and fraudulent documents and personal information has been established around the world [6], with research in Europe and Australia illustrating that the market is organised and punctuated by prolific offenders [9–16]. However, most of this research has focussed on the physical side of the document market, examining documents that are intercepted by police and security organisations. While important, the physical market is only one side of the coin, and previous research has expressed that to properly understand an illicit marketplace, both the physical and digital sides of the market need to be considered [17–19].

Anonymous online marketplaces (also known as cryptomarkets) are, as the name suggests, online marketplaces that use encryption and encrypted currencies to preserve the anonymity of their users. Access to these markets require the use of special protocols, (for example TOR - The Onion Router, or i2P) as these marketplaces are housed in self-regulated spaces of the web, known as the dark web [20,21].

While the online trade of illicit drugs has existed since the 1960s [22], it wasn't until 2011 that the first platform economy for illicit goods and services emerged [20]. Between the years of 2011 and 2013, Silk Road reigned supreme amongst the online anonymous marketplaces, and while the building blocks for its creation already existed, it was the first cryptomarket of its kind, in that its appearance, structure, and organisation were more similar to what was the norm for clear web platform marketplaces like eBay and Amazon. [20]. Over a decade later, this structure is still considered the norm for cryptomarkets.

Since the closure of Silk Road in 2013, there has been a constant state of flux within the cryptomarket ecosystem, with countless new markets opening and subsequently closing due to one of the four main reasons for cryptomarket fatality: intra-market disputes, hacker attacks, exit scams and law enforcement actions [23]. Despite this almost constant state of flux, or perhaps, because of it, the cryptomarket ecosystem has become a criminal environment that exhibits astounding resilience. In the face of targeted and even successful, law enforcement action (which accounts for less than 15 % of market deaths), closures of the dominant marketplaces have no real or lasting impact on the criminal environment [24–27]. If a market is taken down or closed, trade may be temporarily disrupted, but vendors and buyers are quick to adapt, migrating to alternative cryptomarkets, with many vendors operating backup profiles on these competing marketplaces [24,28,29]. It has become apparent that traditional investigative tools are ill-equipped to deal with the resilient and adaptive nature of this criminal environment [28,30]. In recent years, research has had an increasing focus on the intelligence potential of these anonymous online marketplaces, and how they can provide crucial information about the structure and organisation of the trade of illicit goods and services, along with reconstructing the networks of offenders and markets [31]. Admittedly, much of this research has focused on the drug trade [18,27,32–35], due to its dominant nature, but research has expanded to include an examination of the trade of firearms [36–38], counterfeit currency [39], illicit antiquities [40], contracted violence [41], wildlife [42], stolen data [25] and fraudulent identity documents [1,43–45]. The references included here should be considered as examples of this research but are not exhaustive.

While research into the fraudulent document market has been increasing, there is still much that is unknown about this marketplace, even less from an Australian perspective. What has been published about the online market has either largely focussed on vendors operating on the surface web [43], or has served as an introduction to the cryptomarket trade of these products [44,46]. The depth of analysis required to properly understand the cryptomarket facilitated fraudulent document market has not yet been done, with no identifiable research considering the sale of Australian documents specifically. Previous research into the Australian identity crime space [6], and preliminary market analyses [1] have indicated that fraudulent Australian identity credentials are some of the most common products for sale on dark web marketplaces, however this portion of the market has not been explored in detail. Clearly, research into the online marketplace for fraudulent documents could provide key intelligence to assist in disrupting the manufacture, sale, and distribution of these illicit goods. This is especially important for Australian law enforcement to help address the increasing identity crime climate within Australia, an environment with a great financial impact [6,47].

In this research, we aim to provide further insight into the online fraudulent identity document marketplace by examining two anonymous online marketplaces that were both operational between 2018 and 2021, White House Market (WHM) and Empire Market (also referred to as Empire). Both markets were, at the time of their operations, considered top markets within the cryptomarket criminal environment, attracting thousands of vendors and tens of thousands of listings [44,48–52]. In this study both markets will be examined with a specific focus on illuminating the identity-related market, examining its structure, size, and trends in products offered and vendor behaviours. This will be examined first with a focus on the overall identity-related market, before then focusing more on the Australian document market. This research will help to increase the understanding of the fraudulent document market structure, and provide information regarding the manufacture, sale and online distribution of documents internationally, and from an Australian perspective.

2. Materials and methods

2.1. Dataset

The two markets examined in this study are Empire Market and WHM, the details of their operation and the crawl periods are included in Sections 2.1.1 and 2.1.2.

2.1.1. 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 [50,51]. However, by late August 2020, Empire had closed, and it later surfaced that the administrators had exit scammed, stealing approximately $30 million (USD) from its users [53]. Empire was crawled[1] eight times over the period between June and August of 2020, the latest being the 12th of August, shortly before the markets' closure. The webpages of the advertisements were extracted, and then cleaned (i.e. removal of duplicates and blank/incomplete listings), resulting in 79,397 unique listings and 2806 distinct vendors.

2.1.2. 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 [48]. 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 with approximately 900,000 registered users at the time of its closure [52]. During its operation, WHM was crawled 30 times, across eight months of 2020 and three months of 2021. The webpages of the advertisements were extracted, and then cleaned, resulting in 83,517 unique listings, and 2519 distinct vendors.

[1] The automated process of using a computer program to search, collect and index web page content and information [20,54]

2.2. 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, were 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.[2] While the number of sales was available for Empire Market, no such data was provided for WHM, and after initial examinations, it was found that the feedback on WHM was not an accurate representation of the number of ID-related sales. Previous research has illustrated that 60–90 % of the transactions on dark web markets typically receive feedback [27,29,54–56]. To test if these percentages were true of the ID-related market, the three most prolific vendors on Empire (sales) were identified and the number of feedback they obtained on WHM was examined. Collectively, these three vendors only had 43 ID-related feedback, so, given this low number, all sales analyses were limited to Empire Market. 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 [18,29,55,57], which is especially relevant as Empire Market and WHM were contemporaries.

2.3. Classification of listings

The product category as dictated by the vendor was extracted, however, these categories are often incorrect, or not relevant for research [18]. 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 search as previously used in [17–19]. This macro was optimised in this study for the ID-related market, identifying keywords of importance by studying the fraudulent document literature (for example [1,6,43]) along with the product titles of the listings. This classification enabled the extraction of only those items that fell within the ID-related category, including both identity documents and identity fraud-related products. This came to 2545 unique listings and 234 vendors on Empire, and 1620 unique listings and 141 vendors on WHM. The different categories used for the ID-related products can be found in Table A1 in the Appendix.

2.4. Data analysis

2.4.1. Structure of the international market

To illustrate the supply and demand of the ID-related market 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 ID-related market. To provide context, this was also calculated for the overall market, including the illicit drug market. On cryptomarkets, when a vendor runs out of stock of an item, they will often greatly increase its price to dissuade buyers, in some cases indicating in the listing title that they are out of stock [18,29,58]. When this was identified those listings were not included in the price, or the calculations for total value of sales (n=43). The total sales revenue per item, along with the estimated value of the ID-related market on Empire was calculated by first converting the price (in USD or EUR) to AUD as described above, and then multiplying that by the number of sales. The total revenue for every item in the ID-related category was then summed together to estimate the total value of the ID-related market on Empire. This was repeated for the illicit drug market to provide a point of comparison.

Previous research illustrated that the ID-related category had a significant number of listings for digital items [18], so to determine the number of digital listings present on WHM and Empire, the keyword macro used to classify the products 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 U.S. passports). In this instance the macro targeted words associated with countries, states, or regions around the world, including common abbreviations. In some cases, vendors would indicate they were selling documents from a range of countries or regions (e.g. Europe, Asia, Oceania, etc.) which would result in them being classified as ‘Various’. In cases where no document country was included in the listing title, these would be classified as ‘Not Specified’. As these document countries provided no real information regarding the document type, 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 %).

2.4.2. Trafficking of documents

Across both WHM and Empire, vendors indicated their shipping locations, being the places that they ship items from and where they ship to. While it is not possible to verify that this information is accurate, 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 [18,59,60]. 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 [17,60]. Of course, this is largely limited to physical products, given that all digital products are sent to the buyer through the Internet. For these digital products, there is a far higher percentage of vendors selecting ‘Worldwide’ as the origin and shipping country, providing no valuable information about the origins of these products [17]. For this reason, only the physical products have been considered when examining the origin and movement of the ID-related products, and those sales with an origin location of ‘Worldwide’ were removed. On Empire, some vendors indicated a list of countries as potential locations that they would ship to, in which cases the lists were separated to ensure that the countries were correctly represented. This left 189 listings and 552 sales from Empire, and 323 listings on WHM to be analysed. To examine the trafficking of the Australian products, only those items with a document country of Australia were included in the analysis. This left 27 listings (Empire and WHM combined) and 92 sales on Empire to examine.

2.4.3. Vendor behaviours

The number of sales and listings per vendor, in combination with the total value of sales (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 markets, either as a reaction to the closure of a market, or as a strategy to reduce risk [25], and/or to expand their reach thereby increasing their likelihood of higher profits [30,61]. As a vendor’s username is intrinsically tied to their reputation [62], 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 [25,28,30]. However, this uncertainty can be somewhat mitigated by pairing the comparison of the vendors’ username with the comparison of their PGP (Pretty Good Privacy) key [27,63]. After the PGP keys were cleaned to remove formatting inconsistencies between the markets, a vendor username and PGP key comparison was done to identify which vendors were present across both markets.

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

All data analysis was conducted using a combination of Microsoft Excel for Microsoft 365 MSO Version 2401, Tableau 2023.2, and Flourish Studio.[3]

2.5. Ethical considerations

This research work is covered by ethics application number C_FDCA_022022_00009 granted by the University of Lausanne, Switzerland, where the cryptomarket data was crawled. 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 usernames can be identified, all usernames have been anonymised, and no personal information or profile data has been included in this 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. Results and discussion

3.1. Structure of the international identity-related market

In the context of the overall illicit marketplace, on Empire and WHM only 3.4 % and 1.9 % of the listings were for ID-related products and 8.4 % and 5.6 % of the vendors, respectively, were selling products of this kind. This is quite a small portion of the market, especially when compared to other more dominant product categories, such as illicit drugs (49 % and 64 % of the product listings on Empire and WHM respectively). The ID-related category contains a broad range of product types that, for the sake of simplicity, have been grouped into three subcategories that are defined in Table 1. For more detailed definitions of all the product types found within each subcategory, refer to the Appendix Table A1.

Across the ID-related category, there are 2545 listings and 234 vendors on Empire and 1620 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. Understandably, the drug-related categories are largely made up of physical products, while the guides and tutorials, fraud, and ID-related categories have far more digital products on offer [17]. As illustrated in Fig. 1, 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's licences are the most listed products for sale, consistent with previous research [1,6], followed by fullz, then identity fraud packs on Empire, and identity cards on WHM. Driver's 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 [6]. In addition, in some countries driver's licences are attractive as they do not have an expiry date [64].

Table 1
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's 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 (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, rather they can only support a photo ID, or as proof of address	Utility bills, bank statements, birth certificates

While the number of listings is a good indicator of the supply across the market, the sales per item provide an accurate indication of the demand for these products. There were 48,655 ID-related sales on Empire, 95 % of which were for digital products, illustrating that there is both a significant supply (indicated by the number of listings) and demand for digital products within these marketplaces. Interestingly, the category with the highest number of sales, being the identity fraud-related category, is made up entirely of listings for digital products (Table 2). This high number of digital products 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 [6] 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 the recent increases in the trafficking of these precursors [1], indicates that the manufacture of physical documents may be a potential use for these digital documents.

As illustrated in Table 2, the total value of sales across Empire Market for the ID-related category was over $1.8 million (AUD) 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 revenue of $265,303,894 AUD), 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 $426–652 billion USD per annum) [20]. 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 [65–67]. 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 only be responsible for a portion of the fraudulent document market.

In fact, it has been illustrated previously that the fraudulent document market spans the breadth of the dark web, with some storefronts operating outside the jurisdiction of cryptomarkets. These illicit activities are not restricted to the dark web, with a range of activities residing in the domain of the clear web 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 [1,43,45,64,68]. Previous research in Australia has illustrated that clear web storefronts are used by Australian customers to access fraudulent documents, as they linked a commonly encountered

[3] https://flourish.studio/

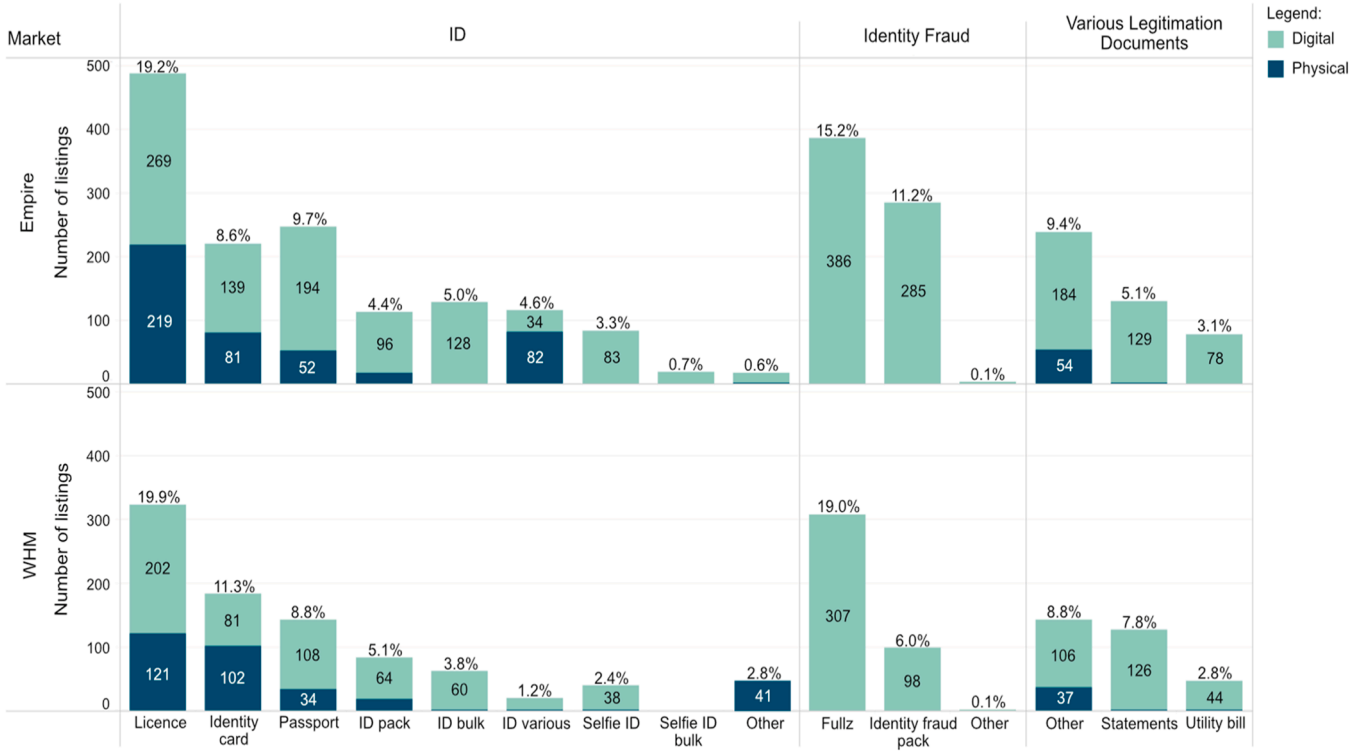

Fig. 1. The number of listings per product type across the ID-related category for both Empire and WHM, with the colours indicating whether the documents are physical (dark teal) or digital (light aqua). The percentage indicates the percentage of listings in each individual market that are for a particular product type (e.g. 19.9 % of listings on WHM are for licences).

Table 2
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	5653	$402,059
	Passport	245	1072	$67,204
	Identity card	212	1164	$189,902
	ID bulk	128	3980	$70,164
	ID various	118	1497	$104,836
	ID pack	111	1024	$65,014
	Selfie ID	83	532	$38,787
	Other	20	125	$14,276
	Selfie ID bulk	18	1	$489
	Total	**1428**	**15,048**	**$952,731**
Identity fraud	Fullz	384	20,649	$435,345
	Identity fraud pack	286	8186	$261,094
	Other	3	336	$18,712
	Total	**673**	**29,171**	**$715,152**
Various legitimation documents	Other	237	2725	$129,480
	Statements	130	1185	$16,388
	Utility bill	77	526	$9735
	Total	**444**	**4436**	**$155,603**
Grand Total		**2545**	**48,655**	**$1,823,485**

clear web storefront selling “novelty identity documents” to those seized by local police [14]. All of this, clearly illustrates that cryptomarkets are not the sole route of access for fraudulent identity documents and stolen personal information, suggesting that the 1.8-million-dollar figure does not illustrate the entirety of the online market, and that the actual value is likely to be higher.

Much research within the document intelligence field has focussed on identifying the structure within the document fraud market by profiling fraudulent documents seized or intercepted by police, identifying those documents that are produced by the same source [9–16,69,70,71]. This research has illustrated that the physical fraudulent document environment is organised and punctuated by prolific offenders [9–16,69,70,71]. Similarly, the identification of these 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 resilient nature of cryptomarkets to disruptions such as police takedowns [20,24,25,27,28], it has been suggested that rather than targeting markets, which are promptly replaced, security and policing organisation should instead consider targeting the more prolific offenders, being those individuals that are having a large impact on the supply and sales within the marketplace [34]. 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.

Fig. 2 illustrates the number of sales per vendor for both the overall market and the ID-related market, to help identify if the presence of prolific offenders, and the structure of the market, is unique to the ID-related market, or if it is instead more likely a symptom of the overall cryptomarket ecosystem. Within the overall and ID-related market on Empire, most vendors (50 % of the overall, and 72 % of the ID-related) are contributing less than 100 sales to the marketplace. Contrasting to this, 460 (16 %) vendors in the overall market, and 13 (5.5 %) vendors in the ID-related market are contributing more than 1000 sales. While this seems to be a small number of vendors exhibiting this prolific behaviour, the extent of their operations is clear when looking at the proportion of the market that they are responsible for. In both cases, these comparatively small groups of vendors are responsible for most of the sales within the markets, with the group of 460 vendors being responsible for 81.6 % of the sales on the overall market, and the 13 ID-related vendors contributing 63.2 % of the sales within the ID-related market. Clearly, this level of concentration and the presence of prolific offenders is not unique to the fraudulent document market 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

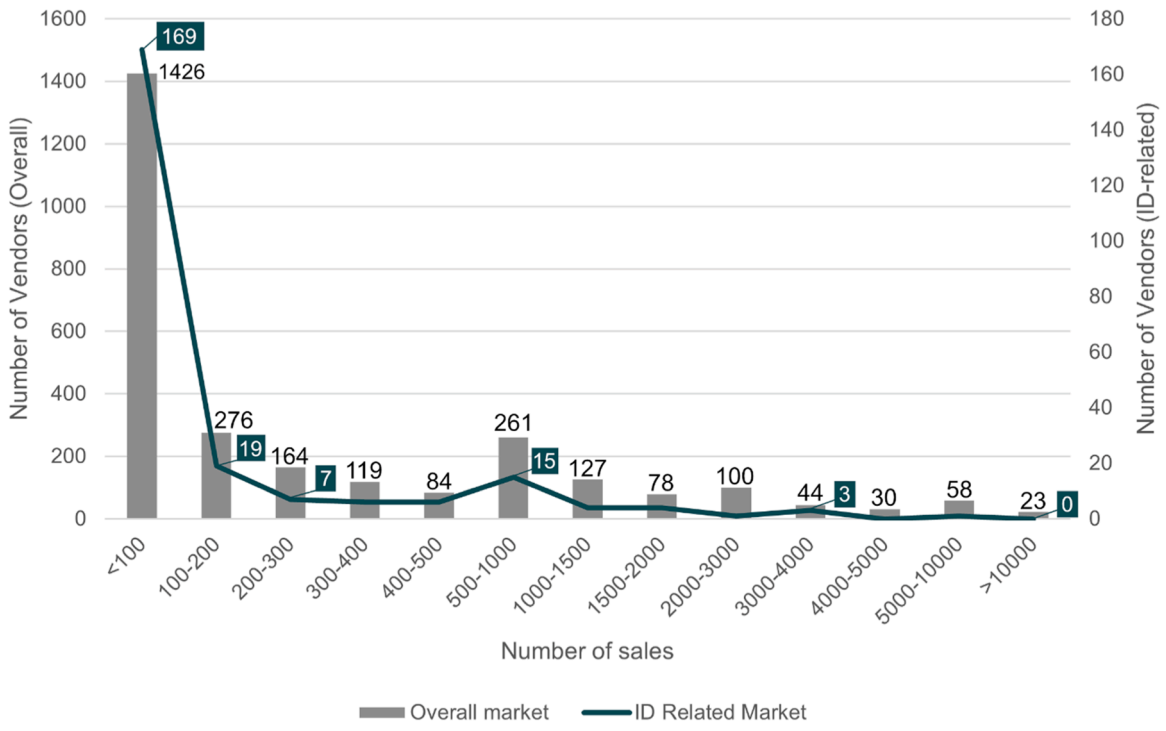

Fig. 2. Number of sales per vendor across the overall (columns) and ID-related (line) market on Empire Market. The columns/line illustrate the number of vendors that have that number of sales (e.g. there are 1426 vendors in the overall market and 169 in the ID-related market with less than 100 sales).

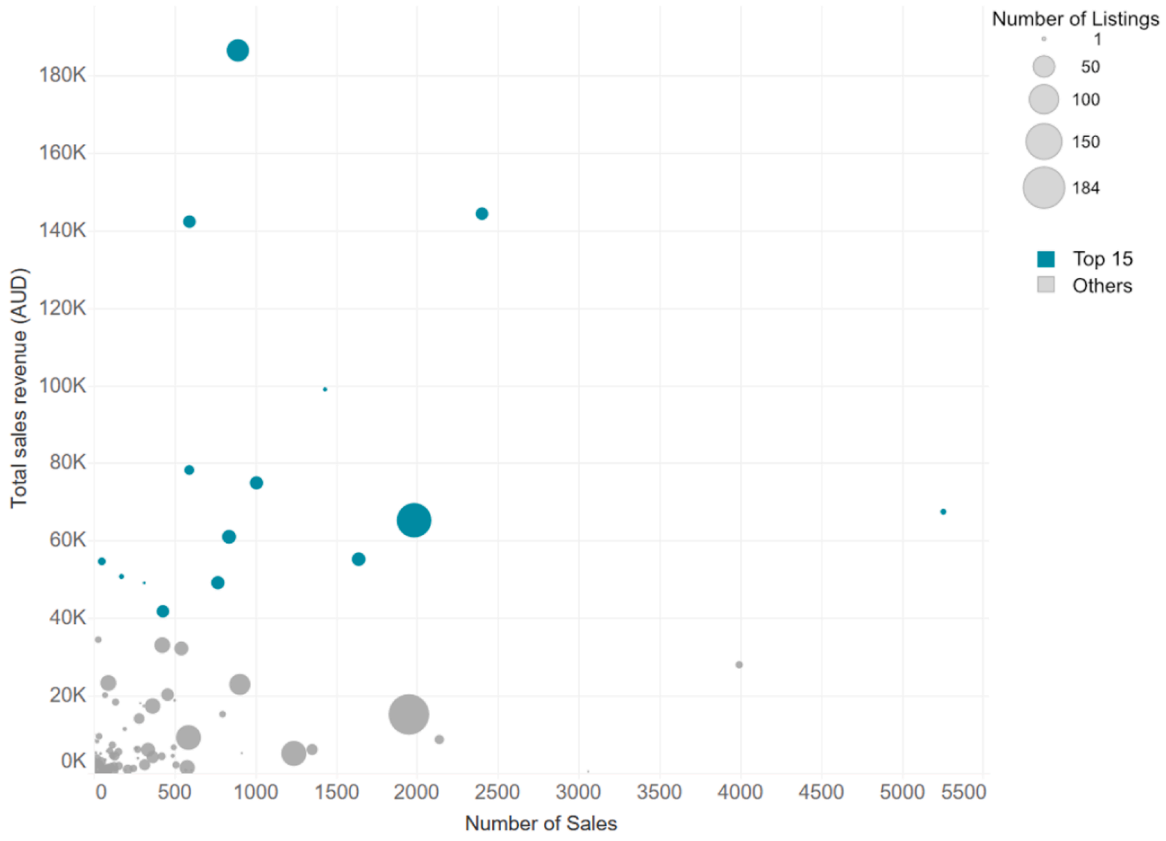

Fig. 3. Total sales revenue (AUD) in regard to the number of sales (x-axis) and listing (size) per vendor with the colour indicating the 15 vendors with the highest total sales revenue.

offending [72].

While the examination of the number of sales per vendor of ID-related products enables the identification of potentially prolific vendors, using the 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 total sales revenue AUD). 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 value of sales when identifying prolific behaviour is illustrated in Fig. 3, which shows the total sales revenue in AUD (highlighting those 15 vendors with the highest sales revenue), along with their number of sales (x-axis) and number of listings (size).

Overall, the proportion of the sales provided by the top 15 vendors is very high, especially given there were 243 ID-related vendors on Empire. 51 % of the market sales are coming from these vendors, while they are only contributing 24 % of the number of ID-related listings. 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 5256 sales coming from six listings, all within the identity fraud-related category. The vendor with the highest total sales revenue is also the vendor with the fourth highest number of sales, and again, a very small number of listings. 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. 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.

3.2. Document country and shipping origin

Examining the country that a document is claiming to be from can provide insight into what types of documents are being targeted by manufacturers, along with what document countries are most popular among buyers. This can 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, along with trends in document fraud and other criminal activities. Of course, previous research has illustrated that the cryptomarket environment is dominated by users from English-speaking and Western European countries [17,18,54,60,73], 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 listings devoted to products of this kind (42.8 % of Empire, and 40.2 % on WHM). 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 United Kingdom (U.K.), followed by Canada and a range of European countries. This trend continues when considering the number of sales, as illustrated in Table 3, with the U.S. again dominating the marketplace. The volume of both sales and listings for U.S. documents and stolen personal information (the identity fraud-related category), is significantly higher when compared to the other document countries (Table 3).

Table 3
Number of sales for each document country across the three ID-related subcategories, and the total sales (%). Only the top 5 contributing countries are illustrated here.

Document Country	Number of Sales				
	ID	Identity fraud	Various Legit.	Total	% of ID Market (total)
U.S.	4719	25,353	1553	31,625	65 %
Australia	1764	595	570	2929	6 %
U.K.	1023	877	219	2119	4 %
Canada	98	443	149	690	1 %
France	487	2	136	625	1 %

Over the last few years, identity crime has continued to rise on an international scale [74,75]. Between 2018–2021, during which Empire and WHM were both active, there was a noted increase in the instances 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 [74]. 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 [74]. 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 6000 working professionals across the U.S., Australia, France, Germany, Italy, and the U.K. This work revealed that 33 % of U.S. respondents had experienced identity theft, which was twice the global average [76].

Given the victimisation rate of identity crime within the U.S., it starts to make more sense why there are so many U.S. products available on these cryptomarkets. It should be noted however, that both the Federal Bureau of Investigation (FBI) and the cybersecurity company that conducted the study 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. Compounding this is the often over-representation of U.S. users, both vendors, and buyers, on English-speaking cryptomarkets, and their much higher population, which may be one of many reasons as to why there are so many more U.S. documents than those from other countries. However, this does not discount the potential for these results and those from the FBI and the previous study [74,76] to be highlighting a potential trend between identity crime and the online ID-related market.

Interestingly, when examining the origin country of vendors selling physical documents, a significant portion of the sales for U.S. (95.7 %), Australian (84.8 %), 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. This is unsurprising, as the ability to manufacture a quality counterfeit or forged document is undoubtedly linked to the manufacturer's familiarity with and access to documents of that kind. A parallel could be drawn between the document market and the illicit drug market in relation to product specialities being dictated by domestic access or familiarity with the items listed, impacted by the origin country of the vendor [60]. Furthermore, selling items within the vendor's country of origin reduces their risk of being detected, with most mail controls and checks being conducted at the borders by customs [18,60].

3.3. Australian documents in the cryptomarkets

Australian documents are the most listed (on WHM and Empire) and the most sold documents (on Empire) after the U.S. This prevalence of Australian documents within the online document market is not anomalous to these two markets, with it being mentioned in previous research [1,77]. Across both Empire and WHM combined there were 294 listings for Australian documents coming from 52 vendors, totalling 7.0 % of the document market. On Empire, there were 2929 sales for Australian documents from 31 vendors, which was 6.0 % of the sales for the ID-related products, with a total sales value of $183,557 (AUD). Overall, within the Australian market, driver's licences and identity (ID)

packs are the products with the most sales.

The popularity of Australian driver's 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 proving the holder's identity and enabling them to fraudulently gain access to more secure documents, such as passports. The 100-point identity check system was introduced in Australia to try and reduce instances of financial fraud [6]. To open an account with a bank or credit union, the customer must hit the 100-point identity threshold, by supplying a range of documents, all of varying degrees of security (and therefore different point values) [6]. From a product perspective, on Empire Market, this 100-point pack (or 'digital wallet') often included a scan of a driver's 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's licences and particularly Australian ID packs are so popular. So much so, that when compared to ID packs from other countries, Australian ID packs have the highest number of sales.

The popularity of Australian driver's licences also exists beyond the cryptomarket ecosystem, with driver's licences being the most commonly misused document as reported by victims of identity crime in 2017, 2019, 2020 and 2023 [6,47,75,78].

3.3.1. *Trafficking of Australian 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. 70 % of the listings for these Australian documents had Australia as the country of origin, with China and the U.S. following behind with 15 % of the listings each (Fig. 4). Similarly, when looking at the number of sales, the domestic nature of the Australian document market is highlighted with 89 % of sales having an origin of Australia, with the other 11 % coming from the U.S. While this suggests the prevalence of the domestic market, it is possible that there are Australian documents being manufactured in and shipped from 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 may be other countries contributing to the Australian document market, but from this analysis, it was not possible to identity them.

The presence of a strong domestic market in Australia is not unique to ID-related products, with previous research indicating that there is also a strong domestic market in Australia for illicit drugs [17,18]. This tendency for vendors to distribute their goods on a domestic scale has been attributed to the general risk-averse nature of vendors and buyers operating on cryptomarkets, with domestic shipments being less likely to encounter parcel loss, interception by authorities, or arrest, especially when dealing with countries that have stronger border controls, such as Australia [17,18,54,60]. 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 [18,60].

Undoubtedly, the geographic isolation of Australia plays a role in the trafficking of any physical illicit goods, along with the general risk-averse nature of vendors leading them to avoid shipping to countries with strict border controls. However, with analysis limited to two markets it is difficult to assess the impact of domestic manufacturing and price. Fig. 4 does suggest that there is domestic shipping, with the majority of the Australian documents originating domestically, and while there have been previous instances of domestic manufacture of these documents [6,79,80], 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 not the opinion of the authors that prices are likely to play a significant role, 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 the low rates of international shipping, and the stronger domestic market.

3.3.2. *Vendor behaviours*

When looking at the vendor behaviour across the listings for the Australian documents on the markets (Fig. 5), 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 to Fig. 5, the sales across Empire are much more concentrated (Fig. 6), with most of the sales being contributed by only a few vendors, with less diversification in their products sold. Fig. 6 illustrates the number of sales per document type, with each colour indicating a different seller. Of the 2929 sales for Australian documents on Empire, 2752 of them (94 %) were for digital documents, with all

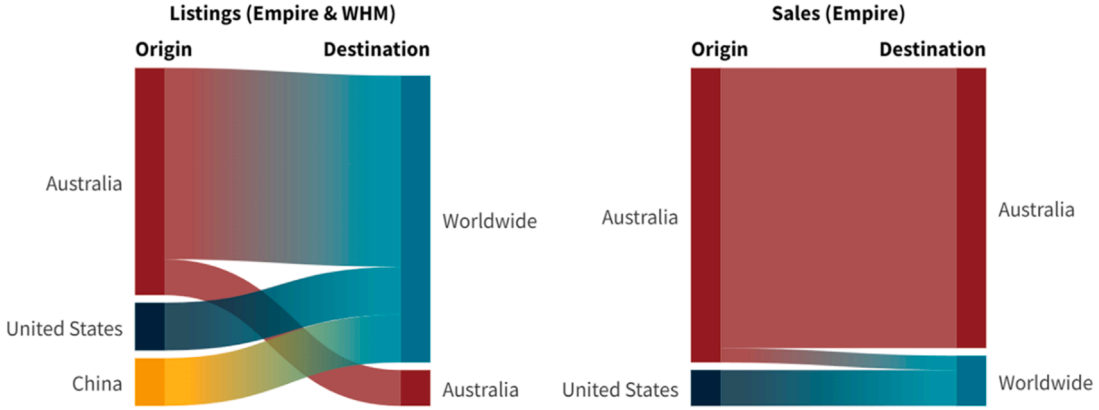

Fig. 4. Trafficking patterns for Australian documents across both Empire and WHM. Listings are on the left, with the number of sales (Empire) on the right.

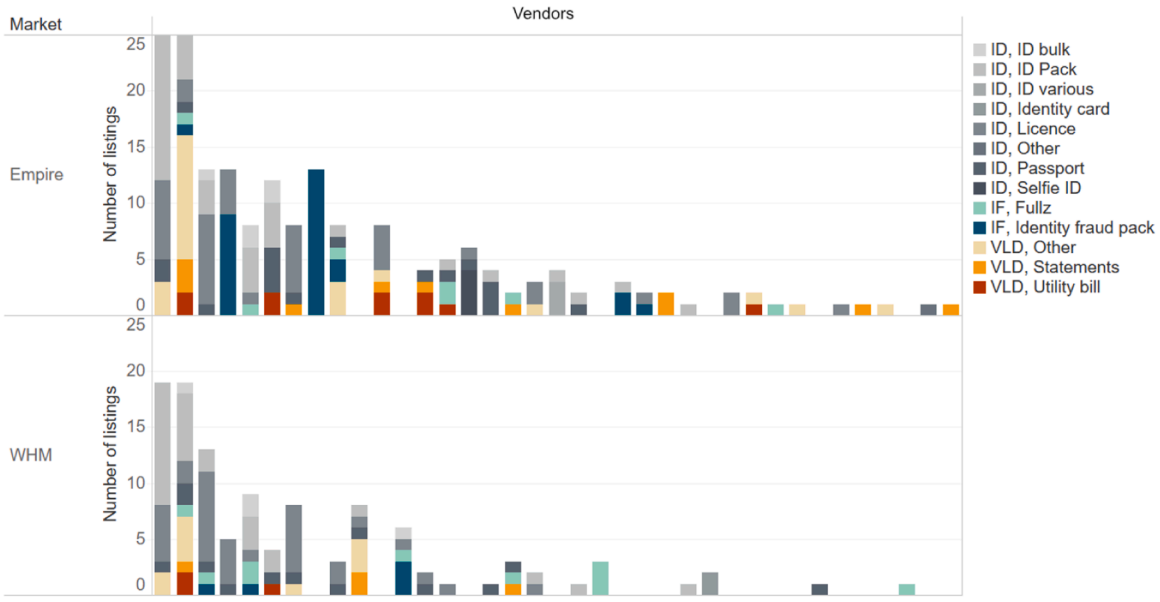

Fig. 5. The number of listings per vendor (Australian documents) across Empire and WHM with the colour indicating the document type and category. Every vendor is depicted as a column along the horizontal axis. For ease, identity fraud has been abbreviated to 'IF' and various legitimation documents has been abbreviated to 'VLD'.

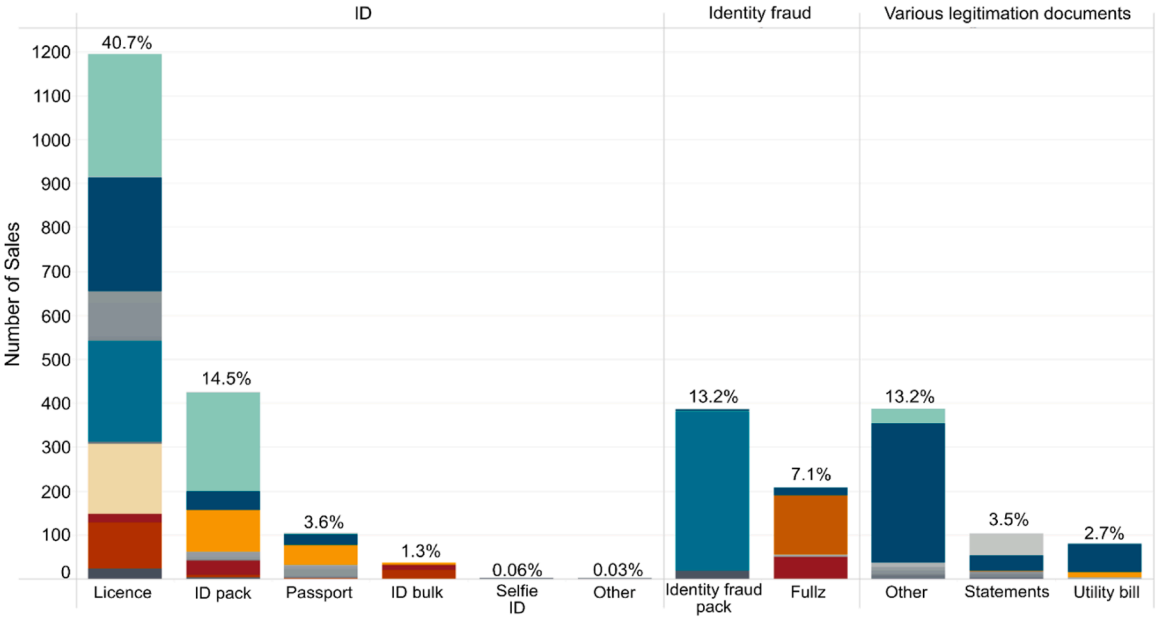

Fig. 6. The number of sales per document type (Australian documents) on Empire. Both physical and digital documents are included here, and each unique colour is indicating a different vendor username.

remaining sales being for counterfeit physical documents, most of which were driver's licences. Overall, considering both physical and digital documents, 40.8 % of the sales for Australian documents were for driver's 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.

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 (AUD) 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 in the grand scheme of the overall market, the three main vendors are contributing 1901 sales to the market, which is 65 % of the Australian document sales. This indicates that the cryptomarket facilitated online market for Australian fraudulent documents is punctuated by prolific offenders, similar to what has been published regarding the physical market [14]. It also appears that these vendors have specialised within the ID-related market, in that they only offer Australian documents, with no other document countries included in their product profiles. This prolific offender analysis points to relevant targets for law enforcement to work on neutralising top contributors to the market.

When comparing the usernames and PGP keys of all ID-related vendors, 18 % of vendors were operating across both Empire and WHM. All three of the vendors discussed as being the top three contributing vendors to the Australian document market, were also

operating across both WHM and Empire.

All sales from the top vendors were for digital documents, except for one, who had 69 sales for one counterfeit driver's licence listing. Upon further analysis it was found that this vendor, 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. Across the overall market on Empire, they have 4825 sales and a total sales revenue of over $1.6million, placing them in the top 30 vendors (out of the 2806 vendors on Empire) regarding sales revenue. This vendor, according to their vendor profile, had 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 would be significantly reduced not just in the ID-related market, but also in the illicit drug market.

4. General discussion and conclusion

In this research, data from two cryptomarkets, Empire and WHM was used to help identify the structure of the online ID-related market, examining trade on both an international and domestic scale, with a specific focus on Australian products. In the larger context of the overall market, the ID-related product category only took up a small percentage of the listings across Empire Market and WHM (3.4 % and 1.9 % respectively), with nearly all listings and sales being for digital products.

On an international scale, the market for U.S. documents was dominant on Empire and WHM, with them being the most listed and sold document country. In particular, there was an abundance of listings within the identity fraud-related category for U.S. fullz and identity fraud packs. While taking up a much smaller percentage of the market, Australian documents were the second most listed, and the second most sold, with driver's licences and ID packs being particularly popular, likely due to the presence of the 100-point identity check system present in Australia [6]. Both the ID-related and Australian document markets were punctuated by a small number of prolific offenders contributing the majority of the sales and listings to the market, similar to what has been identified regarding the physical market for fraudulent documents [9,10,12,13–16,69]. Within the Australian document market, three vendors were identified as being of particular interest, with them contributing over 65 % of the sales for Australian 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 claiming to originate from within the respective country. This suggested the presence of a domestic market, and when looking at the trafficking of Australian documents it was found that most of the sales for Australian documents were being shipped domestically on Empire. The potential reasons behind this domestic market were discussed, with the geographical isolation and strict border controls present in Australia likely deterring the usually risk-averse vendor from shipping to this country. Given the impact that domestic manufacturing has had on the illicit drug market in Australia [18,60], it is not unreasonable to wonder if this is also playing a part in the domestic market for fraudulent Australian documents. However, at this stage, it is impossible to conclude with certainty, to what degree this manufacturing is occurring in Australia. While there have been previous media reports regarding this domestic manufacture [6,79,80], these are from too long ago to be considered an accurate representation of the current criminal environment.

These difficulties with identifying trends in manufacturing and trafficking are intrinsically related to studying an online market dominated by digital products. 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. However, given the presence of 'document precursors' on these cryptomarkets (i.e. components used to make identity documents such as holograms and barcodes), and the recent increases in their trafficking [1], 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.

Of course, the study of any online market, is not without its limitations. The cryptomarket environment, as discussed earlier, is one that is constantly evolving and changing, and the sudden closure of Empire was not something that could be anticipated. This created a clear disparity in the number of crawls (and crawling period) between Empire and WHM. While this did limit the amount of data that was collected for Empire market, each crawl collected every listing that was active at the time of the crawl, including those that had been active since the opening of Empire in early 2018. So, while there were only eight crawls conducted, these provided a good indication of how the market had been operating across these years of activity.

Overall, the information extracted from cryptomarkets, like any trace, is incomplete and therefore needs to be used in partnership with other sources of information. One needs to consider the market as a whole, comprising both online and physical portions before conclusions regarding the manufacture, supply and distribution of goods can be made [17–19]. For the fraudulent document market, this means considering the research and results of the profiling work that has been conducted internationally [9,10,12,13–16,69], and identifying ways that this research can be partnered with examinations of the online fraudulent document market, on both the dark web and the clear web.

So far there has been little research that has actively combined both aspects of the fraudulent document market, treating the online and physical portions of the market as dichotomous. However, this research has illustrated similarities between these two sides of the market, along with the general criminal environment for document fraud and identity crime. Both online and physical markets are characterised by prolific offenders that are contributing significantly to the fraudulent document market. Further examination of the products offered online, either through procuring them, or conducting more active analyses within the currently operational cryptomarkets and open web storefronts, could help identify similarities between the documents in both the online and physical market, resulting in the potential identification of sources, trends in shipping, and manufacture. At the end of the day, much like with the illicit drug market, the online and physical market for identity-related products are two sides of the same coin, and to properly understand the fraudulent document market, they need to be considered as such. 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. It also provides an original and useful perspective on the (supposedly increasing) digitisation of criminal markets.

CRediT authorship contribution statement

Ciara Jean Devlin: Writing – review & editing, Writing – original draft, Visualization, Methodology. **Marie Morelato:** Writing – review & editing, Supervision, Conceptualization. **Simon Baechler:** Writing – review & editing, Supervision. **Quentin Rossy:** Writing – review & editing, Visualization, Supervision, Conceptualization. **Scott Chadwick:** Writing – review & editing, Supervision. **Sébastien Moret:** Writing – review & editing, Supervision.

Declaration of Competing Interest

The authors have no conflict of interest.

Acknowledgements

This work was supported by an Australian Government Research Training Program Scholarship that was awarded to Ciara Devlin.

Appendix

Table A1
Definitions of product types and categories used to group products within the ID-Related market

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 as a means 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 a photo and personal information (e.g. proof of age cards in Australia)
	ID pack	An ID pack is used to describe a collection of one or more documents of different types often curated to serve a specific purpose, such as securing a bank loan or opening a bank account.
	ID bulk	A bulk listing for two or more 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 of 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 drivers licence, passport etc.
	ID component	A building block or 'part' of an identity document to be used in its manufacture e.g. barcodes, security features, and substrates etc. These products were put into the 'other' category for classification, but defined separately here for clarity
	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. card printers)
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 theft, 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, their 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, social security numbers etc.
Various legitimation documents	Statements	This contains all listings that included 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, and insurance cards, residence permits etc.

References

[1] S. Baechler, Document fraud: will your identity be secure in the twenty-first century? Eur. J. Crim. Policy Res. 26 (3) (2020) 379–398, https://doi.org/10.1007/s10610-020-09441-8.
[2] United Nations Office on Drugs and Crime (UNODC), Report of observations and conclusions of the session on the use of forensic sciences to combat and prevent identity-related crime, in Commission on Crime Prevention and Criminal Justice of the United Nations, International Core Group of Experts on Identity-Related Crime, Editor. 2010b, United Nations Office on Drugs and Crime.: Vienna, Austria.
[3] D. Ombelli, F. Knopjes, Documents: The Developer's Toolkit, IOM - International Organisation for Migration Via Occidentalis Editora Lda, 2008.
[4] A. Schloenhardt, Organized crime and the business of migrant trafficking, Crime Law Soc. Change 32 (3) (1999) 203–233, https://doi.org/10.1023/A:1008340427104.
[5] A. Schloenhardt, F. Douglas, J. Lelliott, in: Migrant Smuggling Working Group (Ed.), Stop the planes!? Document fraud and migrant smuggling by air in Australia, The University of Queensland, Brisbane, Australia, 2012.
[6] Jorna, P. and R.G. Smith, Identity crime and misuse in Australia 2017, in Statistical Report no. 10. 2017, Australian Institute of Criminology: Canberra, Australia.
[7] Europol, European Union serious and organised crime threat assessment, A corrupting influence: the infiltration and undermining of Europe's economy and society by organised crime, Publications Office of the European Union, Luxembourg, 2021.
[8] Europol, European Union serious and organised crime threat assessment, Crime in the age of technology, The Hague, The Netherlands, 2017.
[9] S. Baechler, R. Boivin, P. Margot, Systematic processing of false identity documents for crime intelligence purposes: towards a systematic approach, Rev. Int. Criminol. Police Tech. Sci. 68 (2015) 315–337.
[10] S. Baechler, et al., False identity documents profiling: a promising forensic intelligence method to fight identity document fraud, Rev. Int. Criminol. Police Tech. Sci. 64 (4) (2011) 467–480.
[11] S. Baechler, P. Margot, Understanding crime and fostering security using forensic science: the example of turning false identity documents into forensic intelligence, Secur. J. 29 (4) (2016) 618–639, https://doi.org/10.1057/sj.2015.26.
[12] S. Baechler, O. Ribaux, P. Margot, Student paper: toward a novel forensic intelligence model: systematic profiling of false identity documents, Forensic Sci. Policy Manag.: Int. J. 3 (2) (2012) 70–84, https://doi.org/10.1080/19409044.2012.744120.
[13] S. Baechler, et al., The systematic profiling of false identity documents: method validation and performance evaluation using seizures known to originate from common and different sources, Forensic Sci. Int. 232 (1) (2013) 180–190, https://doi.org/10.1016/j.forsciint.2013.07.022.
[14] C. Devlin, et al., The potential of using the forensic profiles of Australian fraudulent identity documents to assist intelligence-led policing, Aust. J. Forensic Sci. 55 (6) (2022) 720–730, https://doi.org/10.1080/00450618.2022.2074138.
[15] S.L. Moulin, C. Weyermann, S. Baechler, An efficient method to detect series of fraudulent identity documents based on digitised forensic data, Sci. Justice 62 (5) (2022) 610–620, https://doi.org/10.1016/j.scijus.2022.09.003.
[16] B. Talbot-Wright, et al., Image processing of false identity documents for forensic intelligence, Forensic Sci. Int. 263 (2016) 67–73, https://doi.org/10.1016/j.forsciint.2016.03.054.
[17] J. Broséus, et al., A geographical analysis of trafficking on a popular darknet market, Forensic Sci. Int. 277 (2017) 88–102, https://doi.org/10.1016/j.forsciint.2017.05.021.
[18] J. Broséus, et al., Forensic drug intelligence and the rise of cryptomarkets. Part I: studying the Australian virtual market, Forensic Sci. Int. 279 (2017) 288–301, https://doi.org/10.1016/j.forsciint.2017.08.026.
[19] M. Morelato, et al., Forensic drug intelligence and the rise of cryptomarkets. Part II: combination of data from the physical and virtual markets, Forensic Sci. Int. 288 (2018) 201–210, https://doi.org/10.1016/j.forsciint.2018.05.002.
[20] J. Martin, J. Cunliffe, R. Munksgaard, Cryptomarkets: A Research Companion, Emerald Publishing Limited, Bingley, 2019.
[21] D. Kavallieros, et al., Understanding the Dark Web, in: B. Akhgar, et al. (Eds.), Dark Web Investigation, Springer International Publishing, Cham, 2021, pp. 3–26.

[22] J. Markoff, What the Dormouse said: How the sixties counterculture shaped the personal computer industry, Penguin Books, 2005.
[23] K. Moeller, R. Munksgaard, J. Demant, Flow My FE the vendor said: exploring violent and fraudulent resource exchanges on cryptomarkets for illicit drugs, Am. Behav. Sci. 61 (11) (2017) 1427–1450, https://doi.org/10.1177/0002764217734269.
[24] J. Van Buskirk, et al., The recovery of online drug markets following law enforcement and other disruptions, Drug Alcohol Depend. 173 (2017) 159–162, https://doi.org/10.1016/j.drugalcdep.2017.01.004.
[25] M. Ouellet, et al., The network of online stolen data markets: how vendor flows connect digital marketplaces, Br. J. Criminol. 62 (6) (2022) 1518–1536, https://doi.org/10.1093/bjc/azab116.
[26] I. Ladegaard, Open secrecy: how police crackdowns and creative problem-solving brought illegal markets out of the shadows, Soc. Forces 99 (2) (2020) 532–559, https://doi.org/10.1093/sf/soz140.
[27] J. Broseus, et al., Studying illicit drug trafficking on Darknet markets: Structure and organisation from a Canadian perspective, Forensic Sci. Int. 264 (2016) 7–14, https://doi.org/10.1016/j.forsciint.2016.02.045.
[28] D. Decary-Hetu, L. Giommoni, Do police crackdowns disrupt drug cryptomarkets? A longitudinal analysis of the effects of Operation Onymous, Crime. Law Soc. Change 67 (1) (2017) 55–75, https://doi.org/10.1007/s10611-016-9644-4.
[29] K. Soska, N. Christin, U. Assoc, Measuring the Longitudinal Evolution of the Online Anonymous Marketplace Ecosystem. Proceedings of the 24th USENIX Security Symposium, 2015, pp. 33–48.
[30] I. Ladegaard, Crime displacement in digital drug markets, Int. J. Drug Policy 63 (2019) 113–121, https://doi.org/10.1016/j.drugpo.2018.09.013.
[31] Q. Rossy, D. Decary-Hetu, Internet traces and the analysis of online illicit markets, in: Q. Rossy, et al. (Eds.), The Routledge International Handbook of Forensic Intelligence and Criminology, Routledge, 2017, pp. 249–263.
[32] M. Chawki, The Dark Web and the future of illicit drug markets, J. Transp. Secur. 15 (3-4) (2022) 173–191, https://doi.org/10.1007/s12198-022-00252-y.
[33] D.S. Dolliver, S.P. Ericson, K.L. Love, A geographic analysis of drug trafficking patterns on the TOR network, Geogr. Rev. 108 (1) (2018) 45–68, https://doi.org/10.1111/gere.12241.
[34] M. Morelato, et al., An insight into prescription drugs and medicine on the AlphaBay cryptomarket, J. Drug Issues 50 (1) (2020) 15–34, https://doi.org/10.1177/0022042619872955.
[35] H.K. Sudan, et al., Decrypting the cryptomarkets: trends over a decade of the Dark Web drug trade, Drug Sci. Policy Law (9) (2023), https://doi.org/10.1177/20503245231215668.
[36] T.J. Holt, J.R. Lee, A crime script model of dark web firearms purchasing, Am. J. Crim. Justice 48 (2) (2023) 509–529, https://doi.org/10.1007/s12103-022-09675-8.
[37] J.R. Lee, T.J. Holt, O. Smirnova, An assessment of the state of firearm sales on the Dark Web, J. Crime. Justice 47 (1) (2024) 46–60, https://doi.org/10.1080/0735648X.2022.2058062.
[38] D. Rhumorbarbe, et al., Characterising the online weapons trafficking on cryptomarkets, Forensic Sci. Int. 283 (2018) 16–20, https://doi.org/10.1016/j.forsciint.2017.12.008.
[39] T.J. Holt, J.R. Lee, E. O'Dell, Assessing the practices of online counterfeit currency vendors, Crime Delinquency (2022), https://doi.org/10.1177/00111287221134047.
[40] K.A. Paul, Ancient artifacts vs. digital artifacts: new tools for unmasking the sale of illicit antiquities on the dark web, Arts 7 (2) (2018), https://doi.org/10.3390/arts7020012.
[41] A.L. Roddy, T.J. Holt, An assessment of hitmen and contracted violence providers operating online, Deviant Behav. 43 (2) (2022) 139–151, https://doi.org/10.1080/01639625.2020.1787763.
[42] O.C. Stringham, et al., The dark web trades wildlife, but mostly for use as drugs, People Nat. 5 (3) (2023) 999–1009, https://doi.org/10.1002/pan3.10469.
[43] T.J. Holt, J.R. Lee, A crime script analysis of counterfeit identity document procurement online, Deviant Behav. (2020) 1–18, https://doi.org/10.1080/01639625.2020.1825915.
[44] C. Degeneve, J. Longhi, Q. Rossy, Analysing the digital transformation of the market for fake documents using a computational linguistic approach, Forensic Sci. Int.: Synergy 5 (2022), https://doi.org/10.1016/j.fsisyn.2022.100287, 100287-100287.
[45] M. Romagna, Cybermarket for forged identity documents: the illegal trade of identity documents on the surface web and in Onionland, Keesing J. Doc. Identity 47 (2015) 12–15.
[46] 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) DOI: 10.1109/ICDMW.2016.0056.
[47] M. McAlister, C. Franks, Australian Institute of Criminology, Editor. Identity crime and misuse in Australia: Results of the 2021 online survey, Australian Government, Canberra, 2021.
[48] M. Chatterjee, The demise of White House Market will shake up the Dark Web. WIRED, Conde Nast, 2021.
[49] Man, N., et al., Trends in the availability and type of drugs sold on the internet via cryptomarkets, January 2020 - Janauary 2021, in Drug Trends Bulletin Series. 2021, National Drug and Alcohol Research Centre, UNSW Sydney: Sydney, Australia.
[50] DarknetStats. Empire Market. 2020 [cited 2023 07/11/2023]; Available from: https://www.darknetstats.com/empire-market.
[51] dnstats. Empire Market. n.d. [cited 2023 07/11/2023]; Available from: https://dnstats.net/site/empire-market/.
[52] C. Cimpanu, Dark web marketplace White House Market shuts down. The Record, 2021.
[53] Power, M., Online Drug Market Empire Disappears, with $30 Million of Users' Money, in Vice News. 2020, Vice: Vice.com.
[54] K. Kruithof, et al., Internet-facilitated drugs trade: An analysis of the size, scope and the role of the Netherlands, RAND Corporation, Santa Monica, CA, 2016.
[55] J. Demant, R. Munksgaard, E. Houborg, Personal use, social supply or redistribution? Cryptomarket demand on Silk Road 2 and Agora, Trends Organ. Crime. 21 (1) (2018) 42–61, https://doi.org/10.1007/s12117-016-9281-4.
[56] R. Munksgaard, et al., Distributing tobacco in the dark: assessing the regional structure and shipping patterns of illicit tobacco in cryptomarkets, Glob. Crime. 22 (1) (2021) 1–21, https://doi.org/10.1080/17440572.2020.1799787.
[57] M.J. Barratt, J. Aldridge, Everything you always wanted to know about drug cryptomarkets (but were afraid to ask), Int. J. Drug Policy 35 (2016) 1–6, https://doi.org/10.1016/j.drugpo.2016.07.005.
[58] M. Paquet-Clouston, D. Décary-Hétu, C. Morselli, Assessing market competition and vendors' size and scope on AlphaBay, Int. J. Drug Policy 54 (2018) 87–98, https://doi.org/10.1016/j.drugpo.2018.01.003.
[59] J. Aldridge, D. Décary-Hétu, Hidden wholesale: the drug diffusing capacity of online drug cryptomarkets, Int. J. Drug Policy 35 (2016) 7–15, https://doi.org/10.1016/j.drugpo.2016.04.020.
[60] J. Van Buskirk, et al., Who sells what? Country specific differences in substance availability on the Agora cryptomarket, Int. J. Drug Policy 35 (2016) 16–23, https://doi.org/10.1016/j.drugpo.2016.07.004.
[61] L. Norbutas, S. Ruiter, R. Corten, Reputation transferability across contexts: maintaining cooperation among anonymous cryptomarket actors when moving between markets, Int. J. Drug Policy 76 (2020), https://doi.org/10.1016/j.drugpo.2019.102635.
[62] S.W. Duxbury, D.L. Haynie, Building them up, breaking them down: topology, vendor selection patterns, and a digital drug market's robustness to disruption, Soc. Netw. 52 (2018) 238–250, https://doi.org/10.1016/j.socnet.2017.09.002.
[63] van Wegberg, R.S. and T. Verburgh, Lost in the Dream? Measuring the Effects of Operation Bayonet on Vendors Migrating to Dream Market', in Web Science Conference '18. 2018: New York, USA.
[64] L. Bellido, S. Baechler, Q. Rossy, The sale of false identity documents on the internet, Rev. Int. Criminol. Police Tech. Sci. 70 (2) (2017) 233–249.
[65] Global Drug Survey (GDS). Global Drug Survey 2018. 2018; Available from: https://www.globaldrugsurvey.com/gds-2018/.
[66] Global Drug Survey (GDS). Global Drug Survey 2019. 2019; Available from: https://www.globaldrugsurvey.com/gds-2019/.
[67] Global Drug Survey (GDS). Global Drug Survey 2021. 2021; Available from: https://www.globaldrugsurvey.com/gds-2021/.
[68] J. Ruey, La vente de faux documents sur Instagram, University of Lausanne: Lausanne, Switzerland, 2018.
[69] M. Auberson, et al., 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 Sci. Int. 260 (2016) 74–84, https://doi.org/10.1016/j.forsciint.2016.01.016.
[70] S. Baechler, Des faux documents d'identité au renseignement forensique: développement d'une approche systématique et transversale du traitement de la donnée forensique à des fins de renseignement criminel, University of Lausanne: Lausanne, Switzerland, 2015.
[71] C. Mireault, et al., What if counterfeit IDs could talk ? Chemical profiling of identity documents, Keesing J. Doc. Identity (2017) 9–12.
[72] J.H. Ratcliffe. Intelligence-Led Policing, 2nd ed, Routledge, 2016.
[73] M.J. Barratt, J.A. Ferris, A.R. Winstock, Safer scoring? Cryptomarkets, social supply and drug market violence, Int. J. Drug Policy 35 (2016) 24–31, https://doi.org/10.1016/j.drugpo.2016.04.019.
[74] Federal Bureau of Investigation (FBI), Internet Crime Report 2021, I.C.C. Center, Editor. 2021.
[75] M. McAlister, et al., Identity crime and misuse in Australia, 2023, Australian Institute of Criminology, 2023.
[76] Wombat Security, *2018* User Risk Report. 2018, Proofpoint Inc.
[77] Romagna, M., The cyber-market of identities: criminological analysis on the illegal market of identity documents within the surface Web and Onionland. 2014, Utrecht University: Utrecht.
[78] C. Franks, R. Smith, Identity crime and misuse in Australia 2019, Australian Institute of Criminology, Canberra, 2020.
[79] C. Vedelago, C. Houston, Fake identities: Buying counterfeit Medicare cards, no questions asked. The Sydney Morning Herald, 2016.
[80] M. Morri, Identity theft: Ruthless gangs use fake driver-licences and Medicare cards for crime sprees. Daily Telegraph, 2017.