DEVIANT BEHAVIOR
https://doi.org/10.1080/01639625.2020.1825915

Routledge
Taylor & Francis Group

# A Crime Script Analysis of Counterfeit Identity Document Procurement Online

Thomas J. Holt[a] and Jin R. Lee[b]

[a]Michigan State University, East Lansing, MI, USA; [b]Michigan State University, East Lansing, MI, USA

**ABSTRACT**

Over the last two decades, researchers explored various aspects of the operational practices of online illicit market operations through the Open and Dark Web for various physical and digital goods. Far less work has considered the presence of counterfeit identity documents for sale within these markets, or the process of advertising, purchasing, producing, selling, and delivering these materials. This study utilized a qualitative crime script analysis of 19 vendors advertising counterfeit documents on the Open and Dark Web, focusing on the advertising, actualization, and delivery of various products. The pricing for various document types and the locations they claim to reflect citizenship of were examined, along with the variations dependent on where the product was advertised. The findings demonstrated that the market for identity documents shared common practices to other online markets, highlighting the value of crime script analyses to understand the distribution of goods through illicit markets generally.

**ARTICLE HISTORY**
Received 25 June 2020
Accepted 15 September 2020

## A crime script analysis of counterfeit identity document procurement online

Criminological scholarship considering offenders as rational actors has generated substantive insight into the process of offending and the situational and foreground dynamics that shape behavior (Clarke 1997; Jacobs 1996; Wright and Decker 1994, 1997). From a routine activities perspective, a motivated offender, suitable target, and absence of guardian must converge in time for crimes to occur (Clarke 1997; Cohen and Felson 1979). Motivated offenders who are predisposed to engage in crime must also feel they are competently equipped with access to sufficient resources necessary to complete an activity (Clarke and Cornish 1985; Cohen and Felson 1979). Substantive research considers the behavioral and attitudinal resources offenders must possess to engage in crime, including emotional control (Cherbonneau and Copes 2006; Jacobs and Cherbonneau 2017; Miller 1998; VanNostrand and Tewksbury 1999) and situational awareness of targets and locations (Clarke and Cornish 1985; Copes and Cherbonneau 2006; Wright and Decker 1994, 1997).

Researchers have also considered the role of so-called facilitatory resources, or objects and tools that simplify the process of offending (Clarke 1997; Ekblom and Tilley 2000). Weapons, like knives or guns, can enhance an offender's capacity to harm or intimidate targets (Miller 1998; Natarajan, Clarke, and Johnson 1995). Similarly, technologies like phones, computers, and the Internet can enable rapid communications between offenders in drug exchanges (Natarajan, Clarke, and Johnson 1995), prostitution (Holt and Blevins 2007; Sanders 2008), and organized offenses generally (Congram, Bell, and Lauchs 2013; Leukfeldt, Kleemans, and Stol 2017). Technological innovations can also improve the quality and capabilities of facilitators over time, enabling offenders to innovate and adapt their behaviors to lower their risk of detection (Ekblom 1997).

**CONTACT** Thomas J. Holt holtt@msu.edu School of Criminal Justice, Michigan State University, East Lansing 48824-1312, United States

One of the underexamined facilitators is forged identity documents (e.g., passports and identity cards), which are inherently valuable for various forms of offending, ranging from financial fraud and identity theft (Ekblom and Tilley 2000; Hutchings and Holt 2015; Lacoste and Tremblay 2003) to status offenses such as the purchase of alcohol or tobacco by underage persons (Martinez, Rutledge, and Sher 2007; Martinez and Sher 2010). Additionally, fraudulent identity documents could be used to engage in misrepresentations of self at border crossings and police interactions to minimize risk (Musco and Coralluzzo 2016; Rudner 2008). Evidence suggests that fraudulent identity documents were historically only available to offenders as a function of their social networks and connections to specialized criminal service providers (Rudner 2008). Their skills in producing functional documents were dependent on specialized tools and resources that were not available to the broader population.

The rise of the Internet and improvements in various technologies, such as photocopiers and scanners, have streamlined the quantity and quality of resources available to produce passports and identity cards (Ekblom and Tilley 2000; Musco and Coralluzzo 2016). Consequently, identity documents are now sold in various gray and black markets operating via websites and online forums (Musco and Coralluzzo 2016). These products appear to constitute a small segment of the overall illicit online market and sell at variable price points (Musco and Coralluzzo 2016). The ability to access fraudulent document providers over the Internet reflects the evolution of offending behavior (Ekblom 1997), as individuals do not need specialized knowledge or social connections to acquire the necessary tools to offend (Cloward and Ohlin 1960). Instead, they only need access to an Internet-connected device and understand how to use a search engine (Copeland et al. 2020; Hutchings and Holt 2015; Mann and Sutton 1998). This has particular salience for our understanding of offending, as access to technology can increase offenders' capacity to engage in various offenses in both virtual and physical spaces. In particular, access to quality document vendors may enable offenders to circumvent existing technologies used to authenticate individual identities (Musco and Coralluzzo 2016; Rudner 2008).

The rise of Internet-based distribution channels for counterfeit identity documents calls to question the roles of vendors and clients in online document markets, as well as the process of advertising, purchasing, producing, selling, and delivering these materials. The current study attempted to address this gap in the literature through a qualitative crime script analysis of 19 vendors advertising counterfeit documents on the Open and Dark Web. The steps involved in the advertising, actualization, and delivery of identity documents were examined in detail, including the pricing for various document types and the range of countries affected. In addition, price of goods were examined cross-nationally, along with the roles that customers could play in facilitating others' access to counterfeit documents. The implications of this analysis for our understanding of facilitatory tools and online markets in furthering physical and cybercrimes are explored in detail.

## Crime script analyses and the rise of online markets

Crime script analyses focus on understanding the essential processes and preparations individuals perform to commit an offense (Clarke and Cornish 1985; Cornish 1994). This framework is intended to capture both the chronological and functional phases by which crimes occur, so as to identify interventions and responses to decrease the likelihood of offending at each potential step (Chiu, Leclerc, and Townsley 2011; Clarke and Cornish 1985; Tompson and Chainey 2011). This form of analysis is derived from the rational choice perspective that focuses on the decision-making processes involved in specific crimes, as well as offenders' recognition of risks and rewards that may be incurred throughout the course of offending (Cornish 1994; Tompson and Chainey 2011). Many of these studies examined economic or acquisitive crimes due to their transactional nature, including robbery (Cornish 1994; Smith 2017), check forgery (Lacoste and Tremblay 2003), counterfeit alcohol sales (Lord et al. 2017), pharmaceutical counterfeiting (Kennedy, Haberman, and Wilson 2018; Lavorgna 2015), the sale of stolen vehicles (Morselli and Roy 2008; Tremblay, Talon, and Hurley 2001), and the sale of personal data via various online markets (Hutchings and Holt 2015).

Crime script analyses often consider the schemata or knowledge that individuals have in order to organize their actions and respond appropriately to others in the course of their actions (Borrion 2013; Cornish 1994). In effect, scripts are a learned set of behaviors and routines that offenders utilize to engage in an action (Hutchings and Holt 2015). Additionally, script analyses examine offending at various levels, including meta-scripts assessing various behaviors that fall under a general crime type, such as domestic violence (Borrion 2013; Cornish 1994). So-called track assessments consider a very specific crime type, such as gas station robberies occurring in specific circumstances (Borrion 2013; Cornish 1994). Researchers have also examined scripts at various stages of implementation in the real world. For instance, potential scripts consider offending responses in hypothetical scenarios; planned scripts examine behaviors that actors have identified they will use in future activities; and performed scripts assess sequences of offender behaviors that have occurred previously (Borrion 2013).

Regardless of the level of analytical abstraction, script analyses typically focus on specific actions occurring in a sequential process. The first phase identifies the actions offenders take to prepare for and enter into an offense setting, such as an environment where a burglary or robbery may occur (Cornish 1994; Wright and Decker 1994, 1997) or an online space (Hutchings and Holt 2015). Such examinations consider both the physical tactics and mental preconditions that may be present to justify involvement (Borrion 2013; Cornish 1994). The next step involves the initiation and actualization of the offense, such as target selection and first contact with that individual or object. Then, the process of doing the offense begins, including the chronological engagement and negotiated interaction with the individual or object, and eventual exit from the encounter upon completion of the transaction or offense (Morselli and Roy 2008). Lastly, some consider the post-offense conditions that must be satisfied on the part of the offender or victim, such as the acquisition and use of goods, drugs, or currency.

Crime script frameworks could add substantive value to our understanding of the processes and practices involved in acquiring fraudulent identity documents, as these practices may have changed with technological innovations. There are two ways that identity documents were typically manufactured by counterfeiters. First, an offender may obtain an existing document which can then be forged or falsified (Musco and Coralluzzo 2016; Rudner 2008). Secondly, individuals may acquire a blank document which can then be manufactured to include data and photos to make the document appear legitimate. Limited evidence suggests the price for these documents can range between 100 USD to over 1,000 USD, though the quality of the forgery and its utility for use at physical borders and in interaction with others should be higher in relation to its cost (Musco and Coralluzzo 2016).

At the same time, there may be differential opportunities to access vendors and document producers based on potential customers' access to technology and their functional awareness of online resources (Herley and Dinei 2010; Hutchings and Holt 2015; Smirnova and Holt 2017; Tzanetakis et al. 2015). For instance, most research related to illicit fraudulent document markets has used information derived from Open Web sites, meaning content can be accessed through traditional web browsers, search engines, and other indexed media (Musco and Coralluzzo 2016). Historically, illicit documents could be purchased through websites run by single vendors, similar to a single-operator retail shop (Musco and Coralluzzo 2016).

A small proportion of vendors also sold product via web forums, which have a structure similar to a retail mall in physical space (Copeland et al. 2020; Smirnova and Holt 2017). The site operators provide a communication space via the forums, where individuals can communicate with one another asynchronously via threaded posts. Vendors create their own thread by posting ads for products, which potential customers respond to by asking questions about the product, or in some cases providing reviews of the quality of the vendor and their services after a transaction is complete (Copeland et al. 2020; Holt 2013; Smirnova and Holt 2017). Since vendor threads exist in parallel, customers could read each thread and make a decision to complete a purchase with a specific vendor based on the information available to them at the time (Holt and Lampke 2010; Smirnova and Holt 2017).

Vendors operating on the Open Web appear to accept unencrypted digital currencies, such as WebMoney, and utilize more readily accessible communication platforms for all manner of illicit products, including instant messaging systems and various unencrypted e-mail platforms. (Hutchings and Holt 2015; Motoyama et al. 2011; Smirnova and Holt 2017). In addition, these vendors may offer a wider range of goods and services from around the world due to their ability to be identified by a truly global audience (Smirnova and Holt 2017; Tzanetakis et al. 2015).

By contrast, vendors can also offer illicit products on the "Dark Web," or the portion of the Internet where websites can only be hosted and accessed using specialized encrypted web browsers (Barratt 2012; Copeland et al. 2020; van Hardeveld, Jan, and Kieron 2017). Much of this content is accessible only through the use of The Onion Router (Tor) network and its specialized Tor Browser (Aldridge and Decary-Hetu 2016; van Hardeveld, Jan, and Kieron 2017). As a result, potential customers may encounter difficulty identifying vendors due to the relatively hidden nature of these services (Smirnova and Holt 2017; Tzanetakis et al. 2015).

Dark Web vendors also have variety in advertising platforms similar to those on the Open Web, as they may sell via single-operator website shops (see Aldridge and Decary-Hetu 2016; Copeland et al. 2020; Holt and Smirnova 2017). There are also so-called cryptomarkets, which operate in a similar fashion to forums, where vendors list their ads in direct competition with others that customers must read and interpret before making purchases (Aldrige and Dearcy-Hetu 2016; Barratt 2012; van Hardeveld, Jan, and Kieron 2017). Despite the structural similarities across both Open and Dark Web sales platforms, there are differences in the ways that transactions are completed by Dark Web vendors. This is most evident in the use of cryptocurrencies, like Bitcoin, to facilitate payments between buyers and sellers in Dark Web markets (Aldridge and Askew 2017; Flamand and David 2019; Moeller, Munksgaard, and Demant 2017; Smirnova and Holt 2017). Additionally, participants in various illicit markets hosted on the Dark Web utilize encrypted e-mail platforms for communication to better hide their activities from others (Aldridge and Askew 2017; Moeller, Munksgaard, and Demant 2017).

The differences in operational practices of these online spaces likely impacts the crime scripts used by both buyers and sellers of identity documents. The ways that vendors advertise their products may vary, with those on the Open Web being less discrete and more overt in the keywords used in the language of their sites to increase the likelihood of appearing in search queries (Hutchings and Holt 2017; Smirnova and Holt 2017). Similarly, there may be observable differences in the global scope of passports and resources sold between Open and Dark Web vendors. Prior research demonstrates differences in the scope of data available for sale in illicit online markets, with financial accounts from more countries available among Open Web vendors compared to those on Dark Web outlets (Smirnova and Holt 2017).

There may, however, be parity in the way customers engage with vendors and the processes needed to complete an order for counterfeit documents similar to what has been observed in illicit online physical goods markets (see Aldridge and Askew 2017; Copeland et al. 2020). For instance, there may be a greater dependence on cryptocurrencies among document vendors operating on Dark Web shops compared to those advertising on the Open Web. Similarly, vendors operating single-operator shops may provide less opportunities for customer feedback compared to those advertising on cryptomarkets or forums. The competitive nature of sales in forums appears to foster informal information-sharing strategies among customers to minimize the risk of purchasing defective products or being cheated by unscrupulous vendors (Holt 2013; Holt and Lampke 2010; Holt, Smirnova, and Hutchings 2016; Motoyama et al. 2011). Vendors operating their own web sites do not have the same degree of direct competition, and have the ability to hide feedback which complicates the process of identifying reliable providers (see Tzanetakis et al. 2015).

These variations highlight the need for researchers to better explore and understand the processes used by individuals to acquire fraudulent identity documents, and their similarities with other online illicit market operations. This knowledge can inform our understanding of the overall impact of technology on specialized offending behaviors generally, as well as provide guidance for targeted interventions to disrupt the open sale of documents writ large.

## Data and methods

To address these questions, this study analyzed 19 market vendors located on the Open (n = 11; 57.9%) and Dark Web (n = 8; 42.1%; see Table 1 for detail). Data collection took place from August 2018 to December 2019 to allow for a large sample of advertisements to be collected. Sites were identified through the use of search protocols through Open and Dark Web browsers using keywords such as "buy identity document fake id passport." To augment the limited results of Dark Web search engines, this study included vendors listed in indexes such as the Hidden Wiki and other cryptomarket listings (n = 3; 15.8%) to identify service providers that had been observed in the past (Copeland et al. 2020; Flamand and David 2019).

This sampling strategy led to a number of vendors, though the majority (n = 16; 84.2%) advertised via single-operator shops operating on websites hosted on either the Open (n = 11; 68.8%) or Dark Web (n = 5 31.2%). A limited number of vendors were identified advertising via cryptomarkets (n = 3; 15.8%), though no Open Web forum vendors were found. It is unclear if this may be a function of our sampling strategy, or a reflection of the limited market for identity documents relative to the much larger online markets observed for drugs (e.g. Aldridge and Askew 2017) and stolen data (Smirnova and Holt 2017). Thus, the convenient nature of this sample may limit its generalizability to all illicit markets operating online.

It should be noted that none of the services offered so-called camouflage or fantasy passports and identity documents (see Brantingham 2007; Musco and Coralluzzo 2016). Any materials claiming an individual's residency to fictitious places or citizenship to nations whose names have changed, such as Rhodesia (which is now Zimbabwe), would fall under this category. It is thought that such identity documents would disable individuals from successfully passing through national borders, as there are lists available that document the place-names associated with such materials (Brantingham 2007; Musco and Coralluzzo 2016). This study's exclusion of such products differs from prior estimates that suggest individuals could obtain fictitious documents from online vendors at various prices (Brantingham 2007; Musco and Coralluzzo 2016).

The dataset was created by saving all pages from each site as html files for analysis. Text and images from each website were then read and coded by hand for qualitative and quantitative analyses by both authors (see Aldridge and Askew 2017; Copeland et al. 2020). Most all the Open Web vendors in this analysis operated multiple page websites, leading the total sample to produce approximately 250 pages of printed content for analysis. A qualitative case study design was employed to consider the practices of both vendors and their customers based on the language provided in their advertisements, as well as

**Table 1.** Descriptive statistics of sample (N = 19).

| Vendor ID | Hosting Location | Advertisement Type |
|---|---|---|
| 1 | Dark Web | Cryptomarket |
| 2 | Open Web | Shop |
| 3 | Dark Web | Cryptomarket |
| 4 | Open Web | Shop |
| 5 | Open Web | Shop |
| 6 | Open Web | Shop |
| 7 | Open Web | Shop |
| 8 | Open Web | Shop |
| 9 | Dark Web | Cryptomarket |
| 10 | Open Web | Shop |
| 11 | Open Web | Shop |
| 12 | Open Web | Shop |
| 13 | Dark Web | Shop |
| 14 | Dark Web | Shop |
| 15 | Open Web | Shop |
| 16 | Dark Web | Shop |
| 17 | Dark Web | Shop |
| 18 | Dark Web | Shop |
| 19 | Open Web | Shop |

any images posted for products (see also Aldridge and Askew 2017; Copeland et al. 2020; Holt 2013; Hutchings and Holt 2015).

Open coding was used to identify common themes across the data and fit into the script processes laid out by Cornish (1994). A particular focus was placed on identifying the common processes of each phase of a scene, including conditions that precipitate or motivate a certain action, as well as conditional behaviors that may result from specific decisions or actions (Hutchings and Holt 2015). Awareness of law enforcement activities was also considered as it may lead to certain actions that minimize detection. In addition, methods of purchase, payment, and distribution of product were explored along with any customer support measures and trust mechanisms used by vendors as indications of actualizing, doing, and exiting activities (Hutchings and Holt 2015). Additionally, the range of products sold by place and any differences in price were examined in detail (Smirnova and Holt 2017). All list prices were converted from their original currency (e.g., Euro, Bitcoin) to the equivalent U.S. Dollar value based on 2019 exchange rate listings. Deviant cases were also highlighted, particularly with regard to their use of affiliate programs, to demonstrate differences in the behaviors of vendors and their customers.

## Findings

This analysis utilized public-facing information provided by vendors in their advertisements on the Open and Dark Web. Similar to previous examinations of online data markets, the nature of the current data forced a focus on the scene of online spaces and the market itself (Hutchings and Holt 2015). Offline scenes were also considered where possible, though they had to be filtered through the lens of vendor commentaries. This analysis also focused on the observed scripts of document vendors, with potential scripts for customers based on hypothetical circumstances where appropriate, as we are unable to assess the scripts of customers in their own words. The findings move through the preconditions of potential customers, initiation and entry into the market, vendor actualization and doing of document creation, and exit scripts of the customer and vendor in detail. Direct quotes from vendors were provided using direct language from each post with all spelling and grammar intact. Usernames and URLs were excluded to provide a modicum of anonymity for users (see also Holt 2013; Hutchings and Holt 2015).

### *Preconditions of potential customers*

Examining advertisements for counterfeit documents demonstrated two key potential preconditions vendors employed to affect customer purchasing: travel and economics. The majority of vendors noted the utility of purchasing their products as a vital way to benefit from travel, as noted in this ad from Vendor 15 stating: "To travel is to live" … If you travel, you achieve everything and that could be only possible if you own "passport". A passport is not only approval to all your international trips, but also an identity proof." Vendor 19 also stated: "For a citizen of a totalitarian country or one that holds a passport with poor visa-free travel it means complete freedom of movement along with the right to live and work in a normal developed society." Vendor 8 made similar comments: "Certain passports enable one to travel visa-free from country to country unrestricted. For example, a European passport enables the owner to visit 26 European countries unhindered as a result of the 1985 Shengen agreement."

Several vendors also emphasized the economic benefits that could be accrued through the purchase and use of fraudulent documents. For instance, Vendor 19 wrote: "A second passport can be your key to reduced taxes and increased asset protection and … allows you to do whatever you want with your money is a truly liberating experience." Vendor 8 similarly noted: "Your country of birth may have a tax system that stifles your earning power, and you may wish to use … what may be the preferential banking systems and tax laws of that country."

An additional precondition noted by one Open Web vendor was the need for identity documents among under-aged individuals in the United States. Since persons under the age of 21 are unable to enter certain bars or purchase alcohol in the United States, having a license or identity document indicating the person is of age would remove such restrictions (Martinez, Rutledge, and Sher 2007; Martinez and Sher 2010). The Vendor emphasized the value of their documents to this effect, stating: "By growing off the underage drinking problem here [in the US}, with it grows the selling and making of ID cards that are scan proofed. Authorities here are already fighting a losing battle, because their approaches just don't work anymore."

Though this language was exceptional, it fits within the overall narrative that customers could benefit from purchasing false credentials. Additionally, it demonstrates a tacit awareness that vendors' products may be used to break the law. Despite this, only two sites indicated the legal risks that customers faced if they used counterfeit documents in certain circumstances. Vendor 11 wrote: "It becomes ILLEGAL when you try to legally use any of the Fake or Novelty documents to obtain legal services like Traveling with a Fake Passport. The Fake passport will not pass any airport scan checks and you will be held for using a Fake document." It is unclear whether this message was intended to indemnify or neutralize any responsibility on the part of the vendors, as observed in other online illicit markets for drugs (see Flamand and David 2019) and cybercrime services (see Holt 2013; Hutchings and Holt 2015). A subtler message was expressed by Vendor 8, stating: "we always advise our clients to let us produce them the Real documents if they legally want to use the document." The emphasis on the legal nature of document use by customers illustrates vendors are aware of and understand certain aspects of the law.

## *Initiation and entry into the market*

The primary script for customers to enter into the online market for counterfeit documents required them to use a web browser and/or Dark Web browser plugin to access the sites where vendors advertise and operate. As noted, the majority of vendors advertised through the Open Web (57.9%), enabling ready access to their page content through search engine queries. Those operating on the Dark Web would have to use either links to known vendors via resources like the Hidden Wiki or attempt to identify ads in existing cryptomarkets offering various drugs, guns, and illicit products (see Aldridge and Decary-Hetu 2016; Copeland et al. 2020; Smirnova and Holt 2017). Customers would then have to read the content of the identified advertisements and make a determination as to what vendor best fit their needs.

The reason a customer decided to purchase through a specific vendor was not clear from the language presented in the current sample of advertisements. One factor may be the perceived level of trust that customers felt in the vendor's claims of reliability and authenticity. Only three of the vendors in this sample provided evidence of customer feedback, though they were all single-operator shops, calling to question the veracity of the posted content. In the absence of customer feedback, several vendors took steps to explain their supposed instrumental actualization process to create documents for customers. These comments demonstrated sourcing and legitimacy of vendors' goods and service capabilities to potential customers.

One key claim made by vendors were ties to coconspirators in government agencies who facilitated access to resources, materials, and document approval. For instance, Vendor 19 stated: "We work directly with Government representatives to deliver a fast & secure process of acquiring your second passport." Similarly, Vendor 14 stated: "I create the require[d] official documents and application for you based on your photo and appearance. I give the documents … to my associate within Department of State Passport Agency in your country." Some vendors specified the tools and resources they used to increase the legitimacy of their claims. For instance, Vendor 11 noted:

> We duly replicate all security features like special paper, watermarks, security threads, intaglio printing, micro-printing, fluorescent dyes, color-changing ink, document number laser perforation, latent image, laser image perforation while producing passports and other related documents.

Vendor 10 similarly noted: "Drivers license have RFID chips. License/I.D are Renewable at any local office in country of issue. Holograms, UV infrared ink and watermarks. Driver's License are registered (DVLA/DMV/IBM)."

Customers' specific document needs also likely shaped their decision to interact with certain vendors. To that end, a total of 1,648 individual products were advertised across this sample of Open and Dark Web vendors. The majority of vendors sold passports (n = 660; 40%), followed by state or national identity cards (n = 415; 25.2%), and driver's licenses (n = 323; 19.6%). Additionally, 10.1% (n = 167) of vendors sold what are referred to as whole sets, meaning a passport, identity card, and driver's license. Lastly, 3.5% (n = 58) sold visas while 1.5% (n = 25) sold other items such as marijuana cards, student IDs, and various foreign language certificates such as TOEFL and IELETS. Open Web vendors were much more likely to sell multiple types of identity documents, particularly passports, identity cards, and driver's licenses. Dark Web vendors were more likely to specialize in selling one form of identification, with the exception of one vendor who offered a range of products.

The emphasis vendors placed on the perceived legitimacy of their products were vital for customers, as they varied in their claims of producing legitimate documentation. A total of 915 (60.2%) items sold by vendors were specified as being either fake or legitimate. Of these items, 422 (46.1%) were fake while 493 (53.9%) were listed as legitimate. The majority of state IDs (56.8%; n = 133; total = 234) and passports (56.7%; n = 246; total = 434) were listed as fake. The majority of driver's licenses (69.9%; n = 100; total = 143) and whole units (100%; n = 94) were listed as being legitimate. In addition, only five total products advertised on the Dark Web listed the legitimacy of their documents, with only one being listed as legitimate.

When segmented by place, the majority (51.2%; n = 843) of products were associated with European or EU member states (see Table 2). A modest number also came from Asian (11.7%; n = 192), South American (8.4%; n = 139), and Middle Eastern (7.2%; n = 119) nations. Additionally, documents for Central American nations (1%; n = 17), the U.K. (2.4%; n = 39), Australia/New Zealand (3.6%; n = 59), Canada (2.4%; n = 39), and Africa (1.2%; n = 20) represented a far smaller segment of the overall proportion of products offered. U.S. documents were a surprisingly small proportion of all countries represented (5.2%; n = 85), with 81.4% (n = 35) of products described by the vendor as being fake. This is in stark contrast to most other nations where there was a reasonably equitable split between fake and legitimate documents sold. Additionally, there were only 43 (2.8%) total instances of individuals selling specific U.S. state identifications/driver's licenses.

The proportion of documents specifically identified as being capable of legitimate use varied by location, with the highest proportion of legitimate goods sold within Central American (71.4%; n = 10) and Middle Eastern nations (69.4%; n = 50). The lowest proportion of legitimate documents appear to originate within the U.S. (18.6%; n = 8). The remainder of locations were almost equally split between fake and legitimate.

**Table 2.** Frequency of items by product type and location (N = 1,648).

| | Driver's License | ID | Passport | Visa | Whole | Other |
|---|---|---|---|---|---|---|
| Africa | 4 | 4 | 9 | 1 | 2 | 0 |
| Asia | 34 | 35 | 90 | 10 | 19 | 4 |
| Australia | 15 | 16 | 19 | 2 | 7 | 0 |
| Canada | 7 | 11 | 16 | 1 | 4 | 0 |
| Caribbean | 4 | 4 | 9 | 1 | 3 | 0 |
| Central America | 3 | 3 | 9 | 0 | 2 | 0 |
| European Union | 178 | 219 | 329 | 26 | 91 | 0 |
| Middle East | 21 | 21 | 53 | 5 | 14 | 5 |
| Mexico | 4 | 4 | 9 | 1 | 3 | 0 |
| Russia | 8 | 7 | 9 | 1 | 3 | 0 |
| South America | 24 | 24 | 72 | 7 | 12 | 0 |
| United Kingdom | 7 | 11 | 15 | 1 | 4 | 1 |
| United States | 13 | 50 | 16 | 1 | 3 | 2 |
| Unspecified | 1 | 6 | 5 | 1 | 0 | 13 |
| Total | 323 | 415 | 660 | 58 | 167 | 25 |

*Note: The frequency of products by type exceeds the total number of product listings (N = 1,521) because numerous ads had individual item listings that fit into multiple product type categories (e.g., "Spain passport + driving license").

Additionally, 49.8% (n = 329) of all advertised passports originated from EU nations, which was the largest concentration of any nation-set. The same pattern was observed for IDs (52.8%; n = 219), driver's licenses (55.1%; n = 178), wholes (54.5%; n = 91), and visas (44.8%; n = 26). In fact, the next largest set of nations represented in passport sales were Asian (13.6%; n = 90) and South American nations (10.9%; n = 72). While the U.S. composed a relatively small proportion of all nations within passport (2.4%; n = 16) and wholes (1.8%; n = 3) advertisements, they were the second largest category for state IDs (12%; n = 50). Asian nations were, however, second in product listing for driver's licenses (10.5%; n = 34), wholes (11.4%; n = 19), and visas (17.2%; n = 10). South American nations were the third highest representation in driver's licenses (7.4%; n = 24) and visas (12.1%; n = 7).

There were also differences in the proportion of countries advertised on the Open Web relative to the Dark Web. A smaller distribution of nations was observed in Dark Web ads, with EU nations and the U.S. were equally represented by vendors at 40% each (n = 18). Only three other locations were specified by vendors: the U.K. (8.9%; n = 4), Russia (4.4%; n = 2) and Canada (2.2%; n = 1). This provides some support for the notion that Dark Web markets feature less global variation than listings posted on the Open Web (Smirnova and Holt 2017).

The observed price for products also varied by location (see Table 3), with EU nations having the greatest variation in price, ranging from 3 USD to 6,496. USD Items from Canada had the highest mean price at 1,533.20, USD followed by the U.K. ($1,480.48) and Australia/New Zealand ($1,394.42). The U.S. had the lowest average price for product at 733.79, USD and was the only country to have a mean price for product under 1,000. USD Products advertised on the Open Web were also substantially higher priced relative to items listed on the Dark Web. For instance, products listed on the Open Web had an average price of 1,299.52 USD compared to 670.22 USD on the Dark Web (see Table 4). The observed difference in price was also statistically significant between Open and Dark Web products generally ($t_{53.550}$ = 5.811, $p$ <.001).

The pricing for products also varied dramatically by vendor and product type (see Table 5). For instance, passports had the greatest variation in pricing, ranging from 10 USD to 10,000, USD with an

**Table 3.** Observed price of products by location in USD.

| | Minimum Price | Maximum Price | Mean Price |
|---|---|---|---|
| Africa (N = 15) | 350.00 | 3,360.00 | 1,356.67 |
| Asia (N = 149) | 350.00 | 6,496.00 | 1,315.07 |
| Australia (N = 53) | 350.00 | 6,160.00 | 1,394.42 |
| Canada (N = 30) | 350.00 | 6,160.00 | 1,533.20 |
| Caribbean (N = 18) | 500.00 | 3,100.00 | 1,223.33 |
| Central America (N = 13) | 600.00 | 3,100.00 | 1,309.23 |
| European Union (N = 687) | 3.00 | 6,496.00 | 1,298.88 |
| Middle East (N = 103) | 500.00 | 3,200.00 | 1,280.52 |
| Mexico (N = 18) | 500.00 | 3,300.00 | 1,273.33 |
| Russia (N = 25) | 2.00 | 3,000.00 | 1,123.02 |
| South America (N = 110) | 350.00 | 3,200.00 | 1,241.65 |
| United Kingdom (N = 32) | 5.00 | 6,160.00 | 1,480.48 |
| United States (N = 74) | 18.00 | 6,496.00 | 733.79 |
| Unspecified (N = 9) | 35.00 | 10,000.00 | 2,194.89 |

*Note: Frequency may not equal total number of product listings (N = 1,521) due to missingness in observed price.

**Table 4.** Observed price of open and dark web products in USD.

| | Minimum Price | Maximum Price | Mean Price |
|---|---|---|---|
| Open Web Products (N = 1,292) | 16.00 | 10,000.00 | 1,299.52 |
| Dark Web Products (N = 44) | 2.00 | 5,000.00 | 670.22 |

*Note: Frequency of products may not equal total number of product listings (N = 1,521) due to missingness in observed price.

Table 5. Observed price of products by type in USD.

| Product Type | Minimum Price | Maximum Price | Mean Price |
|---|---|---|---|
| Driver's License (N = 293) | 5.00 | 5,000.00 | 714.31 |
| ID (N = 391) | 2.00 | 2,240.00 | 562.95 |
| Passport (N = 552) | 10.00 | 10,000.00 | 1,452.28 |
| Visa (N = 57) | 500.00 | 500.00 | 500.00 |
| Whole (N = 167) | 2,500.00 | 6,496.00 | 3,222.47 |
| Other (N = 2) | 59.00 | 5,000.00 | 2,529.50 |

*Note: Frequency of products may not equal total number of product listings (N = 1,521) because of missingness in observed price.

average price of 1,452.28. USD In general, visas had the lowest average price ($500), followed by IDs ($562.95) and driver's licenses ($714.31). Wholes had the highest average price ($3,222.47), which is sensible given the number of items included in the package. Additionally, there were differences observed in the pricing of products on the basis of their advertised legitimacy (see Table 6). Products specified as real or legitimate had a higher mean price ($1,705.02), while those listed as fake were substantially lower ($741.95). Additionally, the observed difference in price was also statistically significant between real and fake products generally ($t_{897.967} = -5.273$, $p < .05$).

## Initiation and entry into the market

Customers initiated transactions after reviewing advertisements and selecting a vendor as with other illicit market purchases (see Aldridge and Askew 2017; Copeland et al. 2020; Flamand and David 2019; van Hardeveld, Jan, and Kieron 2017). This phase of the script begins with first contact between the customer and their preferred vendor, as explained by Vendor 11:

> First, you should start by getting in contact with us, using the contact form on this web page or with the contact details provided on the header and footer of each page our this website. Let us know precisely what your situation is, and what you will need us to provide for you.
>
> -After we receive your message, our support team will get in touch with you directly with all the necessary follow up and complimentary details for the transaction.
>
> -Upon confirmation of the transaction details, we will proceed with the processing of the documents, together with the legal registration and certification depending on the precise document needed and your area or country of jurisdiction.-After document processing, It will be presented to you for verification and validation. We will then proceed with payment for the service, after which your document will then be delivered to you in the quickest notice.

Vendors with online order functionality also allowed customers to submit complete orders electronically. This was explained in the language from Vendor 5's site:

> Simply, there are three things you need to prepare: **1.color certificate photo; 2.ID signature photos; 3.A small amount of bitcoins [to pay for the item]** Once you're ready, you just need to choose the state ID you want to make on the website, fill in the required information step by step, and pay a small amount of bitcoin to complete the order . . . In the store section, click on Buy Fake ID. Edit all the details you want in our fake ID card. You can change your name, date of birth, height, eye color, ID number, signature and upload photos. If there is anything

Table 6. Observed price of products by legitimacy in USD.

| | Minimum Price | Maximum Price | Mean Price |
|---|---|---|---|
| Real Product (N = 414) | 358.00 | 10,000.00 | 1,705.02 |
| Fake Product (N = 368) | 99.00 | 2,240.00 | 741.95 |

*Note: Frequency of products may not equal total number of product listings (N = 1,521) because of missingness in observed price.

> else that needs to be edited on the ID, please fill in your request in Additional info. When all this is done, you can choose to check out or add information about another ID.

Most vendors preferred to engage with customers through electronic means, primarily e-mail platforms. Two vendors provided g-mail addresses, while another two operated a website-based contact form or ticketing system. One used encrypted e-mail via protonmail, a commonly used platform by Dark Web service providers offering various illicit goods (see Aldridge and Askew 2017; Copeland et al. 2020; van Hardeveld, Jan, and Kieron 2017). Six vendors also indicated a phone number for direct contact via voice or text, while one vendor also listed Whatsapp and Skype contacts, respectively.

Vendors also required customers to provide personal information that would be used to create the specific identity document(s) they purchased. The quantity of required information varied by vendor, though most were noted in this ad from Vendor 15: "Your Vital information consists of Your Name, Sex, Date of Birth, Height, etc. And vital information varies depending on the type of document you want us to produce." Customers were also required to provide a photo for all identity document purchases. For instance, Vendor 5 provided a full "Frequently Asked Questions" (FAQ) section for photo production and an image providing exact details to produce the best quality image. The emphasis on a valid and useable photo was also evident in Vendor 15's advertisement, stating: "the photo must be the photo of the person who will be using the document. So the photo must be valid." Otherwise, vendors appeared unconcerned as to whether customers provided legitimate information for document creation.

### *Vendor actualization and doing of document creation*

After a customer initiates contact with a vendor and enumerates their purchase request, the exchange has to be actualized through direct payment. At that time, vendors would engage in the process of document creation. All vendors required payment upfront, which introduces a degree of risk for customers in the event vendors do not deliver as noted in analyses of other online illicit markets (Aldridge and Askew 2017; Copeland et al. 2020; Herley and Dinei 2010; Hutchings and Holt 2015). The majority of vendors preferred electronic payments as they provided immediate, verifiable receipt of currency in exchange for product. Bitcoin (n = 16) and other cryptocurrencies (n = 3) were commonly accepted across vendors regardless of their presence on the Open or Dark Web. Moneygram and Western Union were also accepted by six vendors in keeping with prior analyses of illicit market operations for goods (Holt 2013; Hutchings and Holt 2015; Motoyama et al. 2011). Lastly, three vendors accepted direct wire or money transfer services as payment for goods.

The preference for Bitcoin was made clear by several vendors, due in large part to the overtly illicit nature of their operations. For instance, Vendor 11 explained why it prohibited the use of credit cards and PayPal: "Unfortunately due to the specification of our business it has been difficult accept this payment methods." Vendor 5 was more direct, stating: "It's very simple. It's total anonymous (for you and for us). We are selling fake IDs here and we need a payment method which is anonymous and easy to use. It's really not that difficult to buy bitcoins today."

After receipt of payment, vendors would enact the creation and distribution process from their side. For instance, Vendor 13 stated in their FAQ: "How long does it take to make and ship the IDs? ID cards/drivers licenses about 14 days, passports 21 days." Vendor 5 gave greater detail, including the delivery process stating:

> After completing the order, we will automatically start the production process, and your ID will be ready in about 3-5 days. Then we will send the ID to you by parcel according to the delivery mode you choose in the order. After sending out, we will also provide tracking numbers so that you can inquire about the location of the package at any time, which is so simple and reliable.

A range of shipping options were available to vendors, which could influence delivery times depending on the location of the customer. This was noted in the language from an Open Web vendor (Buy-id.com), stating:

> Delivery time depends on the delivery mode and location you choose in your order . . . Generally speaking, choose DHL express delivery to the United States. Receiving time is only **5-7 days**, if it is in other parts of the world, it will need to increase by 1-2 days. If you choose free delivery, the average time is **7-14 working days**, because the delivery of USPS is always so random. Either way, you can get a tracking number, so everything is under your control.

There was a lack of transparency in most advertisements as to the modes of delivery preferred by vendors, as noted in other studies of online illicit markets for physical goods (Aldridge and Askew 2017; Copeland et al. 2020; Moeller, Munksgaard, and Demant 2017). Three indicated they used DHL, two stated using FedEx and UPS, while only one vendor noted they used the U.S. Postal Service. It is unclear why vendors limited this information in public posts, as it is essential that buyers understand how products will be shipped. This may be a function of operational security for the vendor as these traditional supply chain providers may be more likely to detect or interdict products while in transit. In fact, Vendor 11 noted the need for discretion while shipping in their FAQ section, stating: "**Do any of our company details appear on the document or envelopes they are sent in? Answer**: The documents will be sent in discrete packaging with no reference to our company." Similarly, Vendor 12 noted: "our packages come disguised as a normal letter to make sure it's not intercepted by the courier." Taken as a whole, these comments suggest vendors realized their inherent legal risks for distributing counterfeit identity documents and took steps to shield their operational practices to the extent possible in their ads.

### *Exit scripts of the customer and vendor*

Once delivery information was provided to customers and the product was shipped, the majority of vendors indicated that this satisfied the conditions of their exchange and enabled both parties to exit the script. A few vendors (26.3%; n = 5), however, indicated that they would continue contact with customers in the event their purchases were incorrect or damaged. For instance, Vendor 5 stated: "We give each customer an identical copy free of charge so that they can get two identical fake IDs in one order. because it is not a rare case when people lose or otherwise destroy their card." This was the only vendor to specify they provided a duplicate item free of charge. Instead, four vendors (two from the Open Web and two from the Dark Web) indicated that they would provide product replacements. The specificity of replacement agreements varied, with notes as short as: "yes, there's a replacement time of 10 days. That means, you will get a new one." Another vendor provided a much more detailed paragraph elaborating the various conditions associated with a return, including notifying the vendor by e-mail within one calendar day of receipt of the product, and that the purchase must be received by the vendor within five calendar days of initial delivery. Such detailed language was exceptional, as the general lack of replacements or refunds mirrors prior research on other illicit market operations on the Dark Web (Aldridge and Askew 2017; Hutchings and Holt 2015).

Four sites in this sample also indicated their willingness to continue engaging with customers to effect transactions over time. Specifically, these four vendors operated discount programs to repeat customers as a means to increase sales and offer discounts to regular customers. One of these programs was a simple discounting scheme, as explained in Vendor 5's FAQ section: "I want to order lots of fake documents, can I get a discount? Answer: According our discounting policy you will get 5% discount for your second order, 10% – for 3–4th and 5 or more – 15%." Such language and deals are consistent with other online illicit market strategies intended to retain long-term customers, including credit card data (Hutchings and Holt 2015), malicious software (Holt 2013), and illegal drugs (Aldridge and Askew 2017).

Three other vendors offered so-called affiliate programs, or schemes designed to allow customers to monetize their knowledge of the vendor by driving customers to their site. Two of these were operated through Dark Web sites, as with this language from Vendor 16 that stated:

> Tell others about this shop, and earn 1% from every purchase they will make. Simply give them this link: [removed] Replace YOURUSERNAME with your actual username on this site and get earnings directly to your wallet.

The other was run through an Open Web site using a more complex set of schemes. The first was a relatively simple program to offer referral discounts, stating: "1) share your offer link to a friend, 2) whey they sign up, they get a 25 USD voucher, 3) when they successfully purchase an id with the coupon, you will receive a 25 USD reward." The second scheme was far more involved, and turned customers into vendors operating as resellers for the site. They specifically targeted college students who could sell fake IDs in large quantities to enable underage youth to access local bars, using language such as "Are you currently enrolled in college, around a college, or just know a ton of people who want Fake IDs? Read more to see how it works and how to be a partner."

Anyone who wanted to become an affiliate was required to either deposit 1,000 USD into their personal account on the site or place an order for 10 state identity cards. At that time, the individual is authorized as a reseller for 30 days and entitled to a discounted per-unit price for documents: "according to different states, get a wholesale price of 35-50 USD per ID!" Individuals could retain their reseller status so long as they logged at least five identity document purchases per month. Additionally, resellers were entitled to "global express delivery" with goods arriving within four to 6 days of completion.

The inherent value of becoming an affiliated reseller lay in the ability to charge customers whatever price they see fit. The site specifically noted this in their description of why someone would become a reseller, stating: "In a word, there are too many college students or international students who join us and earn a lot of money. Don't envy them driving luxury cars and hugging beautiful women. You can too." Though a reseller could charge any amount they saw fit, the site noted: "The happier your customers are, the more likely they are to tell their friends that they know where to get an ID. We recommend charging 50, USD but some people charge as much as 200 USD!" Though such an act would seem illegal, the Vendor utilized language that helped minimize potential risk and presented the process as exceedingly easy, explaining:

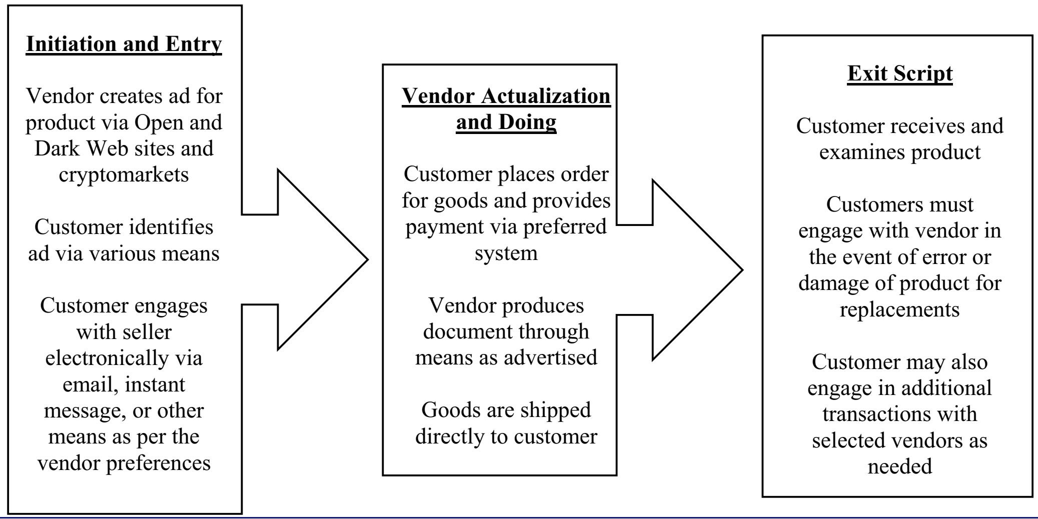
> The dealer's job is actually very simple. You should first get information about each customer: name, birthday, eye color, hair color, weight, height, gender, etc. Most importantly, read the photo instructions to make sure that each of your customers has taken a good picture! Make a clear record of which state ID each customer needs, and then charge the customer a fee. The profit depends on the price you sell. After doing this, you just need to place an order on the website to complete the work.

Such a program was the exception in this analysis, though it is somewhat similar to operations observed in drug cryptomarkets (Aldridge and Decary-Hetu 2016). As a whole, this reinforces the transformative nature of online markets in simplifying offender scripts generally (see also Hutchings and Holt 2015; Mann and Sutton 1998).

## Discussion and conclusions

Extant research demonstrates that criminal offending patterns evolve with technology (Holt and Blevins 2007; Hutchings and Holt 2015, 2017; Leukfeldt, Kleemans, and Stol 2017; Natarajan, Clarke, and Johnson 1995; Sanders 2008). This analysis attempted to address this issue through an examination of crime scripts utilized by vendors and customers engaged in the acquisition of fraudulent identity documents via online markets. Using a sample of 19 vendors, the qualitative findings demonstrated that the process of acquiring fraudulent documents has been simplified by the development of e-commerce style shops that provide on-demand access to personalized identity documents (see Table 7; Musco and Coralluzzo 2016).

Table 7. Summary of crime script process of fraudulent identity document creation.



**Initiation and Entry**

Vendor creates ad for product via Open and Dark Web sites and cryptomarkets

Customer identifies ad via various means

Customer engages with seller electronically via email, instant message, or other means as per the vendor preferences

**Vendor Actualization and Doing**

Customer places order for goods and provides payment via preferred system

Vendor produces document through means as advertised

Goods are shipped directly to customer

**Exit Script**

Customer receives and examines product

Customers must engage with vendor in the event of error or damage of product for replacements

Customer may also engage in additional transactions with selected vendors as needed

The script identified in this analysis demonstrated identity document vendors and their customers follow a process mirroring that of traditional e-commerce behaviors generally (see Table 7). Vendors created advertisements for products, which would be identified by potential customers on the basis of their perceived needs and products of interest. A potential customer would have to initiate a transaction with a vendor to enable vendor actualization and document creation. Upon distribution of product and receipt of goods, both vendors and customers could then affect their exit script, or begin a longer-term relationship depending on their needs and the practices of the vendor.

In fact, the language presented in advertisements demonstrated vendors understood the primary reasons potential customers may have for purchasing identity documents – namely, to misrepresent oneself for travel or economic purposes. In some respects, this mirrors prior research regarding the ways fraudulent documents are used by offenders in the wild (Martinez and Sher 2010; Rudner 2008). Targeted marketing toward college students to enable underage drinking was also an isolated but clear justification for purchasing fake documents (Martinez and Sher 2010). There was less explanation provided by vendors as to their motivations for selling and manufacturing fraudulent documents. Similarly, the inherent legal risks associated with the use of fake identity documents was largely dismissed from advertisements. Instead, vendors seemed to place that onus onto their customers, a pattern which has been observed among other illicit market operations such as the sale of personal information (Hutchings and Holt 2015) and firearms (Copeland et al. 2020).

The information provided by vendors regarding their actualization of document creation suggested they had affiliations to insiders for materials and documentation processing. Furthermore, vendors appeared to have the printing equipment needed to produce documents that match the genuine articles, or at least reasonable facsimiles (Musco and Coralluzzo 2016). These comments suggested vendors have deep access to internal systems and personnel within government agencies, corroborating what has been historically known about document production (Musco and Coralluzzo 2016) and other forms of counterfeiting (Chiu, Leclerc, and Townsley 2011; Kennedy, Haberman, and Wilson 2018; Lavorgna 2015; Lord et al. 2017).

Additionally, detailing the actualization and doing of document production could serve as linguistic signals of legitimacy for customers who must determine what vendor best suits their needs in a competitive online marketplace (Aldridge and Askew 2017; Holt, Smirnova, and Hutchings 2016; Hutchings and Holt 2015). Several scholars have argued that the number of vendors active in diverse online markets may complicate the decision-making process for buyers (Herley and Dinei 2010; Hutchings and Holt 2015; Tzanetakis et al. 2015). Thus, vendors who appear to provide legitimate products and services may seem preferable for buyers who desire the best return on their investment, regardless of whether they operate on the Open or Dark Web (Aldridge and Askew 2017; Smirnova and Holt 2017).

At the same time, this information may have been falsified by vendors in an attempt to sway customers toward their businesses, similar to what has been observed within both stolen credit card (Holt, Smirnova, and Hutchings 2016) and malware markets (Holt 2013). The lack of feedback provided by customers also calls to question how reputable products may be, as customer feedback has been an essential resource for independent validation of sellers and their products (Aldridge and Askew 2017; Holt, Smirnova, and Hutchings 2016; Moeller, Munksgaard, and Demant 2017; Smirnova and Holt 2017). Further study is needed to validate any claims made by vendors and assess the qualities of manufactured goods relative to online claims.

The findings also demonstrated vendors' dependence on cryptocurrencies, regardless of whether they operated on the Open or Dark Web (Aldridge and Decary-Hetu 2016; Copeland et al. 2020; Moeller, Munksgaard, and Demant 2017; Smirnova and Holt 2017). The price for products also varied substantially across document types, location, legitimacy of product, and Open/Dark Web advertising, similar to variations noted in the sale of personal information (Herley and Dinei 2010; Holt and Lampke 2010; Smirnova and Holt 2017) and drugs on the Dark Web (Aldridge and Decary-Hetu 2016). It is unclear whether identity document prices accurately reflect the quality of goods across vendors, or are a technique called "setting a holding price" to deter customers from making purchases the vendor cannot fulfill (Aldridge and Decary-Hetu 2016; Soska and Christin 2015). Further research is needed to disentangle the factors affecting pricing relative to product quality and vendor legitimacy (Copeland et al. 2020).

Taken as a whole, these findings demonstrate that the market for identity documents is similar to other black-market processes observed within stolen data markets (Hutchings and Holt 2015) and online drug sales (Aldridge and Askew 2017). Additionally, this analysis reinforces broader arguments regarding the role that technology has in affecting an evolution in both offending and offenses generally (Clarke and Cornish 1985; Ekblom and Tilley 2000; Mann and Sutton 1998). Not only does the rise of online markets simplify the overall acquisition script for fraudulent documents, but also enables low or unskilled offenders with access to formerly closed-off networks of skilled facilitators (Clarke 1997; Ekblom 1997). In addition, by offering customers the potential to become distributors and indirect advertisers, online markets can engender greater diffusion of knowledge and monetary rewards from illicit activities (Aldridge and Decary-Hetu 2016).

This analysis also highlighted various potential points of intervention to disrupt the online supply chain for documents via online sources (Hutchings and Holt 2017). First, given that more than half of all ads came from the Open Web, it would appear relatively easy to identify vendors. Internet Service Providers (ISP) could generate warning banners noting the illegality of using fake identification for official purposes whenever individuals utilize keyword searches that point to illicit identification sites (Hutchings and Holt 2017). Similar strategies have been employed with individuals seeking hacking service providers, all of which reduced visits to the corresponding websites (Collier et al. 2019). Such strategies may deter potential customers by removing any excuse that they did not know the use of documents was illegal, as well as increasing the perceived risk of purchasing the product to offend, thereby lowering the overall market demand for products (Clarke 1997; Hutchings and Holt 2017).

The lack of feedback mechanisms for customers supported prior research that vendors operating their own shops have greater control over the information available to potential customers to assess their legitimacy (e.g., Copeland et al. 2020; Smirnova and Holt 2017). The lack of public feedback and general reputation systems suggests vendors may not be affected by the use of slander or Sybil attacks that directly manipulate customer trust structures to create confusion among market actors (Copeland et al. 2020; Holt and Lampke 2010; Hutchings and Holt 2017). Instead, law enforcement agencies may benefit from creating convincing websites to increase the perceived overall number of vendors operating online at any time. Additionally, investigators could regularly change the listed prices, range of products available, and from what regions of the world they represent (Copeland et al. 2020). Not only would this increase a vendor's perceived number of competitors, but also increase the perceived difficulties inherent in competing against other sellers (Clarke 1997). In addition, this would increase the perceived complexity of decision-making among potential customers, possibly reducing their willingness to engage in a transaction with anyone (Hutchings and Holt 2017; Tzanetakis et al. 2015).

There are, however, a number of limitations that may affect the findings of this analysis. First, this study was based on advertisements derived from both Open and Dark Web sources, though it is not clear if there may be others vending product in markets that are closed or invitation-only. Thus, these findings may not be generalizable to those market operations. In addition, this study utilized the language provided in postings by vendors which may not accurately reflect all processes and practices (Copeland et al. 2020; Hutchings and Holt 2015). It is possible that some advertisements may have been posted by law enforcement attempting to conduct undercover operations (Hutchings and Holt 2017). Alternatively, advertisements may be posted by fraudsters attempting to generate revenue through the sale of faulty products (Aldridge and Askew 2017; Holt 2013; Hutchings and Holt 2015). Thus, consistent exploratory analyses of the market for identity documents is essential to quantify changes in the supply and demand for products, as well as shifts in their scripted behavior and scenes over time.

## Disclosure statement

No potential conflict of interest was reported by the authors.

## Funding

This work was supported by the Department of Homeland Security under Grant 17STCIN00001-02-00. The opinions and findings expressed are those of the researchers and not of the funding agency, its employees, or staff.

## Notes on contributors

*Thomas J*. **Holt** is a Professor in the School of Criminal Justice at Michigan State University, and its Director. His research focuses on computer hacking, malware, and the role of the Internet in facilitating all manner of crime and deviance. He received his PhD from the University of Missouri-St. Louis in 2005.

*Jin Ree Lee* is a PhD student in the School of Criminal Justice at Michigan State University. His research interests are in cybercrime, online interpersonal violence, cybersecurity, cyberpsychology, computer-mediated communications, and big data.

## References

Aldridge, Judith and Decary-Hétu. David. 2016. "Cryptomarkets and the Future of Illicit Drug Markets." *The Internet and Drug Markets* 21: 23–32.

Aldridge, Judith and Rebecca Askew. 2017. "Delivery dilemmas: How drug cryptomarket users identify and seek to reduce their risk of detection by law enforcement." *International Journal of Drug Policy* 41:101–09. doi: 10.1016/j.drugpo.2016.10.010

Barratt, Monica J. 2012. "Silk road: ebay for drugs." *Addiction* 107 (3):683–683. doi: 10.1111/j.1360-0443.2011.03709.x

Borrion, Hervé. 2013. "Quality assurance in crime scripting." *Crime Science* 2 (1):6. doi: 10.1186/2193-7680-2-6

Brantingham, Barney. 2007. "The camouflaged passport advantage," *The Independent* March , 27.

Cherbonneau, Michael and Heith Copes. 2006. "'Drive It like You Stole It': Auto theft and the illusion of normalcy." *British Journal of Criminology* 46 (2):193–211. doi: 10.1093/bjc/azi059

Chiu, Yi-Ning, Benoit Leclerc, and Michael Townsley. 2011. “Crime script analysis of drug manufacturing in clandestine laboratories: Implications for prevention.”.” *The British Journal of Criminology* 51 (2):355–74. doi: 10.1093/bjc/azr005

Copeland,, Christopher, Mikaela Wallin, and Thomas J. Holt. 2020. “Assessing the practices and products of darkweb firearm vendors.”*Deviant Behavior* 41: 949–968.

Clarke, Ronald V. 1997. *Situational Crime Prevention: Successful Case Studies. 2nd Ed.* Guilderland, NY: Harrow and Heston.

Clarke, Ronald V. and Derek B. Cornish. 1985. “Modeling offenders’ decisions: A framework for research and policy.” *Crime and Justice* 6:147–85. doi: 10.1086/449106

Cloward, Richard A. and Lloyd E. Ohlin. 1960. *Delinquency and Opportunity: A Theory of Delinquent Gangs*. Glencoe, IL: Free Press.

Cohen, Lawrence E. and Marcus Felson. 1979. ““Social change and crime rate trends: A routine activity approach.” *American Sociological Review* 44 (4):588–608. doi: 10.2307/2094589

Collier, Ben, Daniel R. Thomas, Richard Clayton, and Alice Hutchings. 2019. “Booting the booters: Evaluating the effects of police interventions in the market for denial-of-service attacks.” In *Proceedings of the Internet Measurement Conference* 50–64. Amsterdam, NL.

Congram, Mitchell, Peter Bell, and Mark Lauchs. 2013. *Policing Transnational Organized Crime and Corruption: Exploring the Role of Communication Interception Technology*. United Kingdom: Palgrave Macmillan.

Copes, Heith and Michael Cherbonneau. 2006. “The key to auto theft: Emerging methods of auto theft from the offenders’ perspective.” *British Journal of Criminology* 46 (5):917–34. doi: 10.1093/bjc/azl001

Cornish, Derek B. 1994. “The procedural analysis of offending and its relevance for situational prevention.” *Crime Prevention Studies* 3:151–96.

Décary-Hétu, David, Masarah Paquet-Clouston, and Judith Aldridge. 2016. “Going international? Risk taking by cryptomarket drug vendors.” *International Journal of Drug Policy* 35:69–76. doi: 10.1016/j.drugpo.2016.06.003

Ekblom, Paul. 1997. “Gearing up against Crime: A dynamic framework to help designers keep up with the adaptive criminal in a changing world.” *International Journal of Risk Security and Crime Prevention* 2:249–66.

Ekblom, Paul and Nick Tilley. 2000. “Going Equipped.” *British Journal of Criminology* 40 (3):376–98. doi: 10.1093/bjc/40.3.376

Flamand, Claudia and Décary-Hétu. David. 2019. The Open and Dark Web. Pp. 60-80, in *The Human Factor of Cybercrime* Rutger Leukfeldt and Thomas J. Holt (Eds.). London: Routledge.

Herley, Cormac and Florêncio. Dinei. 2010. “Nobody Sells Gold for the Price of Silver: Dishonesty, Uncertainty and the Underground Economy.” Pp. 33–53 in *Economics of Information Security and Privacy*. Boston, MA: Springer.

Holt, Thomas J. 2013. “Examining the Forces Shaping Cybercrime Markets Online.”.” *Social Science Computer Review* 31 (2):165–77. doi: 10.1177/0894439312452998

Holt, Thomas J. and Eric Lampke. 2010. ““Exploring stolen data markets online: Products and market forces.” *Criminal Justice Studies* 23 (1):33–50. doi: 10.1080/14786011003634415

Holt, Thomas J. and Kristie R. Blevins. 2007. ““Examining sex work from the client’s perspective: Assessing Johns using on-line data.” *Deviant Behavior* 28 (4):333–54. doi: 10.1080/01639620701233282

Holt, Thomas J., Olga Smirnova, and Alice Hutchings. 2016. “Examining signals of trust in criminal markets online.” *Journal of Cybersecurity* 2 (2):137–45.

Hutchings, Alice and Thomas J. Holt. 2015. “A crime script analysis of the online stolen data market.” *British Journal of Criminology* 55 (3):596–614.

Hutchings, Alice and Thomas J. Holt. 2017. “The online stolen data market: Disruption and intervention approaches.” *Global Crime* 18 (1):11–30. doi: 10.1080/17440572.2016.1197123

Jacobs, Bruce A. 1996. “Crack Dealers’ apprehension avoidance techniques: A case of restrictive deterrence.” *Justice Quarterly* 13 (3):359–81. doi: 10.1080/07418829600093011

Jacobs, Bruce A. and Michael Cherbonneau. 2017. “Nerve management and crime accomplishment.” *Journal of Research in Crime and Delinquency* 54 (5):617–38. doi: 10.1177/0022427817693037

Kennedy, Jay P., Cory P. Haberman, and Jeremy M. Wilson. 2018. “Occupational pharmaceutical counterfeiting schemes: A crime scripts analysis.” *Victims & Offenders* 13 (2):196–214. doi: 10.1080/15564886.2016.1217961

Lacoste, Julie and Pierre Tremblay. 2003. “Crime and innovation: A script analysis of patterns in check forgery.” *Crime Prevention Studies* 16:169–96.

Lavorgna, Anita. 2015. “The online trade in counterfeit pharmaceuticals: New criminal opportunities, trends and challenges.” *European Journal of Criminology* 12 (2):226–41. doi: 10.1177/1477370814554722

Leukfeldt, Rutger, Edward Kleemans, and Wouter Stol. 2017. ““The Use of Online Crime Markets by Cybercriminal Networks: A View from Within.”.” *American Behavioral Scientist* 61 (11):1387–402. doi: 10.1177/0002764217734267

Lord, Nicholas, Jon Spencer, Elisa Bellotti, and Katie Benson. 2017. “A script analysis of the distribution of counterfeit alcohol across two European jurisdictions.” *Trends in Organized Crime* 20 (3–4):252–72.

Mann, David and Mike Sutton. 1998. “NETCRIME: More change in the organization of thieving.” *The British Journal of Criminology* 38 (2):201–29. doi: 10.1093/oxfordjournals.bjc.a014232

Martinez, Julia A. and Kenneth J. Sher. 2010. "Methods of "Fake ID" obtainment and use in underage college students." *Addictive Behaviors* 35 (7):738–40. doi: 10.1016/j.addbeh.2010.03.014

Martinez, Julia A., Patricia C. Rutledge, and Kenneth J. Sher. 2007. "Fake ID ownership and heavy drinking in underage college Students: Prospective findings." *Psychology of Addictive Behaviors* 21 (2):226–32. doi: 10.1037/0893-164X.21.2.226

Miller, Jody. 1998. ""Up It Up: Gender and the accomplishment of street robbery." *Criminology* 36 (1):37–66. doi: 10.1111/j.1745-9125.1998.tb01239.x

Moeller, Kim, Rasmus Munksgaard, and Jakob Demant. 2017. "Flow My FE the vendor said: Exploring violent and fraudulent resource exchanges on cryptomarkets for illicit drugs." *American Behavioral Scientist* 61 (11):1427–50.

Morselli, Carlo and Julie Roy. 2008. "Brokerage qualifications in ringing operations." *Criminology* 46 (1):71–98. doi: 10.1111/j.1745-9125.2008.00103.x

Motoyama, Marti, Damon McCoy, Kirill Levchenko, Stefan Savage, and Geoffrey M. Voelker. 2011. "An analysis of underground forums." In *Proceedings of the 2011 ACM SIGCOMM Conference on Internet Measurement Conference* 71–80. Berlin, Germany.

Musco, Stefano and Valter Coralluzzo. 2016. "Sneaking under cover: Assessing the relevance of passports for intelligence operations." *International Journal of Intelligence and CounterIntelligence* 29 (3):427–46. doi: 10.1080/08850607.2016.1148477

Natarajan, Mangai, Ronald V. Clarke, and Bruce D. Johnson. 1995. "Telephones as facilitators of drug dealing." *European Journal on Criminal Policy and Research* 3 (3):137–53. doi: 10.1007/BF02242934

Rudner, Martin. 2008. "Misuse of passports: Identity fraud, the propensity to travel, and international terrorism." *Studies in Conflict & Terrorism* 31 (2):95–110. doi: 10.1080/10576100701812803

Sanders, Teela. 2008. "Male sexual scripts: Intimacy, sexuality and pleasure in the purchase of commercial sex." *Sociology* 42 (3):400–17. doi: 10.1177/0038038508088833

Smirnova, Olga and Thomas J. Holt. 2017. "Examining the geographic distribution of victim nations in stolen data markets." *American Behavioral Scientist* 61 (11):1403–26.

Smith, Martha J. 2017. "Expanding the Script Analytic Approach Using Victim Narratives: Learning about Robberies of Taxi Drivers from the Drivers Themselves." Pp. 77–98 in *Crime Prevention in the 21st Century,* Benoit Leclerc and Ernesto U Savona (Eds.). Cham: Springer.

Soska, Kyle and Nicolas Christin. 2015. "Measuring the Longitudinal Evolution of the Online Anonymous Marketplace Ecosystem." In *24th {USENIX} Security Symposium* 15: 33–48. Washington DC.

Tompson, Lisa and Spencer Chainey. 2011. "Profiling illegal waste activity: Using crime scripts as a data collection and analytical strategy." *European Journal on Criminal Policy and Research* 17 (3):179–201. doi: 10.1007/s10610-011-9146-y

Tremblay, Pierre, Bernard Talon, and Doug Hurley. 2001. "Body switching and related adaptations in the resale of stolen vehicles. script elaborations and aggregate crime learning curves." *British Journal of Criminology* 41 (4):561–79. doi: 10.1093/bjc/41.4.561

Tzanetakis, Meropi, Gerrit Kamphausen, Bernd Werse, and Roger von Laufenberg. 2015. "The transparency paradox. Building trust, resolving disputes and optimising logistics on conventional and online drugs markets." *International Journal of Drug Policy* 35:58–68. doi: 10.1016/j.drugpo.2015.12.010

van Hardeveld, Gert, Craig Webber Jan, and O'Hara Kieron. 2017. "Deviating from the cybercriminal script: Exploring tools of anonymity (Mis) used by carders on cryptomarkets." *American Behavioral Scientist* 61 (11):1244–66. doi: 10.1177/0002764217734271

VanNostrand, Lise-Marie and Richard Tewksbury. 1999. "The motives and mechanics of operating an illegal drug enterprise." *Deviant Behavior* 20 (1):57–83. doi: 10.1080/016396299266597

Wright, Richard T. and Scott H. Decker. 1994. *"Burglars on the Job: Streetlife and Residential Break-ins.* " Boston, MA: Northeastern University Press.

Wright, Richard T. and Scott H. Decker. 1997. *Armed Robbers in Action: Stickups and Street Culture*. Boston, MA: Northeastern University Press.