Article

Assessing the Practices of Online Counterfeit Currency Vendors

Crime & Delinquency
1–22

DOI: 10.1177/00111287221134047
journals.sagepub.com/home/cad
SAGE

Thomas J. Holt[1], Jin R. Lee[2], and Elizabeth O'Dell[1]

Abstract

The development of the Internet and e-commerce tools have simplified the process of commercial exchange for both legal and illicit goods. The rise of online markets for illicit goods enable access to facilitatory resources for crime, such as firearms and counterfeit identity documents. Few have considered how these online markets facilitate the sale of counterfeit currencies for use in offline environments. The current study attempted to address this gap in the literature through a qualitative crime script analysis of counterfeit currency vendors operating on both the Open and Dark Web to understand the ways vendors advertise, actualize, and exit these transactions. The implications of this analysis for our understanding of the acquisition processes of facilitatory products are explored in detail.

Keywords

Dark Web, counterfeit currency, online illicit market, crime script, cybercrime

Introduction

Criminals have readily adopted the Internet, including e-commerce websites, advertising tools, and payment platforms, as a means to engage in various forms of illicit exchange. There is substantive research on the use of the

[1]Michigan State University, East Lansing, USA
[2]George Mason University, Fairfax, VA, USA

Corresponding Author:
Thomas J. Holt, School of Criminal Justice, Michigan State University, 655 Auditorium Road, 434 Baker Hall, East Lansing, MI, 48824, USA.
Email: holtt@msu.edu

Internet to sell various products, including malicious software (Holt, 2013; Meland et al., 2020), hacking tools and services (Liggett et al., 2020; Meland et al., 2020), and stolen credit and debit card data (Ablon et al., 2014; Holt & Lampke, 2010; Holt, Smirnova, & Chua, 2016; Lee, 2021). Similarly, there have been myriad studies exploring the growth of online markets selling illicit narcotics on the Dark Web, which is generally described as the part of the web that can only be accessed using specialized browsers such as The Onion Router (Aldridge & Décary-Hétu, 2016; Barratt & Aldridge, 2016; Décary-Hétu et al., 2016).

There has been less research exploring the online markets that enable the sale of facilitatory resources (i.e., tools that simplify the process of offending) to engage in crime (Clarke, 1997; Ekblom & Tilley, 2000; Kruisbergen et al., 2019). For example, few studies have noted the rise of illicit firearms markets hosted on the Dark Web, which provide actors with access to weapons that can be used for criminal purposes in offline spaces (Copeland et al., 2020; Holt & Lee, 2022b; Lee et al., 2022; Paoli et al., 2017). Similarly, limited research has noted the sale of counterfeit identity documents (e.g., passports and driver's licenses) in online illicit markets, which are quintessential for various forms of offending, ranging from financial fraud and identity theft (Ekblom & Tilley, 2000; Holt & Lee, 2022a; Hutchings & Holt, 2015) to the unauthorized purchase of alcohol or tobacco by underage persons (Martinez et al., 2007; Martinez & Sher, 2010).

This type of research is essential to our understanding of crime and criminal behavior, as facilitatory resources such as counterfeit identity documents were historically produced by specialized creators who could only be accessed through established social network ties (Kruisbergen et al., 2019; Rudner, 2008). The growth of various technologies, including printing and digital photography, have streamlined the process of creating fraudulent identity documents and other counterfeit products whose utility hinges on perceived legitimacy (Ekblom & Tilley, 2000; Musco & Coralluzzo, 2016).

To that end, few studies have explored the degree to which counterfeit currencies are available for purchase in the online illicit marketplace. The production of counterfeit money is an illegal activity that has been in practice since forms of currency were first distributed (Finlay & Francis, 2019; Klein et al., 2004; Prime & Solomon, 2010). The use of counterfeit currencies are illegal and can violate numerous state and federal laws depending on the circumstances. At its core, counterfeit currencies undermine the value of the currency it imitates and can lead to economic inflation due to a reduction in value of legitimate currency. Various governments have developed unique methods of detecting counterfeit currency, including the use of unique paper, holograms, and watermarks. The degree to which counterfeiters have been

able to continue producing fraudulent notes have led businesses to develop effective tools (e.g., special markers and scanning tools) to identify counterfeit bills during potential transactions (Judson & Porter, 2010; Prime & Solomon, 2010).

The prevalence of counterfeit currencies and their variability in quality calls to question how offenders gain access to these fraudulent notes. Some argue that technologies like photocopiers and scanners make it easier for offenders to produce counterfeit currency on their own (Ekblom & Tilley, 2000). Additionally, the preponderance of markets in online shops and forums may provide offenders with access to quality counterfeits with minimal effort (see Holt & Lee, 2022a). This highlights an important evolution in offending behavior (Ekblom, 1997), as actors only need access to the Internet to identify sellers and subsequently acquire counterfeit bills (Hutchings & Holt, 2015; Mann & Sutton, 1998). In turn, they may be able to engage in fraudulent purchases more efficiently using these counterfeit bank notes.

The current study attempted to address this gap in the literature through a qualitative analysis of counterfeit currency vendors operating on both the Open and Dark Web. A crime script analysis was applied to understand the process by which illicit vendors advertise, actualize, and exit these transactions. The findings demonstrated variations in the practices of vendors relative to the platforms they used to advertise their products, though there was some parity in the process of vending relative to other illicit products sold in online markets. The implications of this analysis for our understanding of the acquisition process of facilitatory products are explored in detail.

Counterfeit Currencies

Counterfeit currency has been in circulation for as long as physical currency has existed. Some of the earliest forms of counterfeit currency date back to 3,300 to 2,000 BC with cowrie shells, an African currency that was counterfeited using clam shell, stone, ivory, bone, and bronze. More modern forms of currency, such as early paper banknotes and metal coins, were also subject to forgery throughout history. Currency called "jiaozi" in China's Song Dynasty were counterfeited in the 10th century despite strict government restrictions on who could use and access the currency. Greek coins were also frequently counterfeited around 400 BC by taking genuine coins of low value (e.g., copper) and filling them with molten metal (Finlay & Francis, 2019).

The United States Treasury (2006) has identified three basic methods of counterfeit United States (U.S.) currency production: (1) digital printing, (2) traditional offset printing, and (3) intaglio and typographic printing. Digital printing is conducted using computers, scanners, and copying machines.

While this method of counterfeiting requires very little skill, the quality of fraudulent notes is inconsistent. Despite variations in quality, many of the forged notes are still "passable" and may go undetected by the average consumer and retail worker. Contrary to digital printing, traditional offset printing requires specialized equipment and a higher level of skill. With this method, counterfeiters utilize very particular printing equipment to transfer images from etched metal plates to the desired printing surface. Intaglio and typographic printing methods most closely resembles the practices employed by the U.S. Bureau of Engraving and Printing (BEP) to create authentic notes. Counterfeiters adopting this method use specially manufactured paper that more closely mirrors genuine U.S. currency. Currency produced using these methods are often labeled as "supernotes" as they are considered highly deceptive. Despite their superior quality, these fraudulent notes are unable to regularly circumvent financial institutions' detection systems (United States Treasury, 2006).

The method of production that an individual chooses to employ seems to vary depending on the skillset and location of the counterfeiter. For instance, traditional offset lithography is commonplace in South American countries where counterfeiting is typically performed by skilled craftsmen or artisans using traditional, old-fashioned printing presses. In Colombia, counterfeiters take photographs of authentic notes and etch them onto steel plates which are then printed onto genuine $1 banknotes (Finlay & Francis, 2019). Most counterfeit U.S. banknotes (approximately 60%), however, come from Peru. The country is also known to create the most realistic counterfeit U.S. currency, which the U.S. Secret Service has labeled the "Peruvian note." Creating a counterfeit note in Peru can take several weeks to produce, with up to a dozen people playing a unique role in its production. In fact, the individual who prints the counterfeit note is often different from the person who re-creates the texture of the note. Everyone involved in the process is typically unknowledgeable about who else is involved or how they are involved in the overall production (Holley, 2016).

Counterfeiters in the U.S. mostly utilize the digital printing method, using advanced digital and printing technology when producing forged banknotes (United States Treasury, 2006). As a result, counterfeiters do not need considerable amounts of artistic skill to create fraudulent money that would mislead consumers and retailers. Counterfeiters will often take low-denomination banknotes such as the $1 or $5 bill, then bleach it and use advanced technology to print images of $50 or $100 notes over the genuine currency to give it an authentic look and feel (Chase, 2019). In the European context, the EUR 20 and EUR 50 bank notes are the most popular denominations for counterfeiters, accounting for 83% of the counterfeit notes detected in 2015 (Europol,

n.d.). These types of counterfeit bills are unable to bypass detection equipment used by banks, though they can deceive the average consumer and retail worker. Since the currency will not be found to be fraudulent until it is taken to the bank, the financial damage to the business or individual has already been done (Holley, 2016). As a result, several tracking equipment and tools have been developed by Europol to detect counterfeit Euro currency, including a mobile toolkit that provides immediate technical support and expertise in detecting illegal print and markings (Europol, n.d.).

Crime Script Analyses

Despite the prevalence of counterfeiting behaviors, limited criminological inquiry has explored the processes by which individuals produce or acquire counterfeit currencies. The growth of the online marketplace has transformed the ways individuals access counterfeit products of all types, including luxury goods (Perez et al., 2010), pharmaceuticals (Kennedy et al., 2018; Lavorgna, 2015), and identity documents (Holt & Lee, 2022a). It is feasible that online markets are now being used to sell counterfeit currencies for use in offline environments, though few have considered these illicit vendors' operational practices using empirical data.

One way to systematically understand both counterfeit currency production and acquisition is through the application of crime script analyses, which provides a comprehensive framework of the processes and preparations needed to commit various forms of crime (see Clarke & Cornish, 1985; Cornish, 1994). Crime scripts are based on the rational choice perspective that suggests offenders engage in crime by weighing the risks and rewards stemming from their actions (Cornish, 1994; Tompson & Chainey, 2011). These studies largely focus on the learned behaviors and routines that individuals develop in order to structure their behaviors appropriately to each situation in the course of an offense (Borrion, 2013; Cohen & Felson, 1979; Cornish, 1994; Hutchings & Holt, 2015). Based on these findings, policymakers are able to develop formal and informal intervention strategies that reduce the number of offenses at various points in the chronology of an offense (Chiu et al., 2011).

Crime script scholars have explored the procedural scripts for various forms of crime at different levels of analysis. For instance, meta-scripts have been used to assess the overall characteristics of a broad type of offending, such as domestic violence (Borrion, 2013; Cornish, 1994). Researchers have also explored specific crime types using track assessments to assess the practices of gas station robberies (Cornish, 1994). Others have developed potential or planned scripts based on offenders' practices in both hypothetical and real circumstances (Borrion, 2013), including sex trafficking (Brayley et al., 2011).

These analyses focus on the specific and sequential processes of an offense, usually beginning with the actions needed to prepare for and enter into an offense. This includes the mental processes and physical practices needed to negotiate the setting of the offense, whether in physical (Borrion, 2013; Cornish, 1994; Wright & Decker, 1994, 1997) or virtual space (Holt & Lee, 2022a; Hutchings & Holt, 2015). The next step in most crime scripts identifies the initiation and actualization of the offense, which typically involves the process of target selection. The "doing" of the offense then begins, documenting the steps whereby the offender engages in a negotiated interaction with the individual or object, ending with the exit of the offender and any other parties from the scene (Morselli & Roy, 2008). Finally, some scripts assess the post-offense conditions that occur, including the acquisition and use of stolen goods, drugs, currency, or other aspects specific to the offense type (e.g., Holt & Lee, 2022a; Wright & Decker, 1994, 1997).

Many researchers have applied crime script analyses to economic or acquisitive crimes because of their transactional nature (Cornish, 1994; Morselli & Roy, 2008). Recent studies have explored the sales practices of online illicit vendors to understand the mechanics of the offense, including the sale of counterfeit identity documents (Holt & Lee, 2022a), counterfeit pharmaceuticals (Kennedy et al., 2018; Lavorgna, 2015), and stolen personal data (Hutchings & Holt, 2015). This form of analysis improves our understanding of the ways counterfeit currencies are trafficked on e-commerce platforms across the Internet. The strength of this research is in its ability to improve both formal and informal mechanisms to disrupt the commercial exchange of illicit goods and services.

Data and Methods

This study utilized a sample of 18 vendors advertising counterfeit currencies between 2018 and 2020, including 17 shops and 1 cryptomarket from the Open ($n=4$) and Dark Web ($n=14$; see Table 1 for details). A total of 243 counterfeit currency products were advertised for sale across the 18 online vendors within the current sample (see Table 2 for details). The research protocol underwent institutional ethics review and was deemed non-human subjects as there was no immediate way to identify the real identities of the participants or operators. In addition, coded data were stored using unique identifiers to minimize any risk of attribution to specific vendors.

Data collection took place from August 2018 to February 2020 to ensure a broad and comprehensive list of both vendors and product advertisements were captured (see Holt & Lee, 2022a, 2022b). Shops were identified using keywords and phrases such as "fake euro dollars buy shop" on both Open

Table 1. List of Vendors and Market Type ($n = 18$).

Market ID	Market type	Platform
1	Shop	Open Web
2	Shop	Open Web
3	Shop	Open Web
4	Shop	Open Web
5	Shop	Dark Web
6	Shop	Dark Web
7	Shop	Dark Web
8	Shop	Dark Web
9	Shop	Dark Web
10	Shop	Dark Web
11	Shop	Dark Web
12	Shop	Dark Web
13	Shop	Dark Web
14	Shop	Dark Web
15	Shop	Dark Web
16	Shop	Dark Web
17	Shop	Dark Web
18	Cryptomarket	Dark Web

Table 2. Distribution of Product Advertisements by Market Type and Platform ($n = 243$).

	Dark Web	Open Web
Shop	191	45
Cryptomarket	7	0
Total	198	45

and Dark Web search engines (see Appendix for additional details). In addition, the research team examined various Dark Web indexes, such as the Hidden Wiki, to identify vendors that had been observed in the past (Copeland et al., 2020; Flamand & Décary-Hétu, 2019). Cryptomarkets were identified using the same strategy, though the research team attempted to identify all vendors offering counterfeit currencies for sale within each market. Each identified vendor was captured once during the data collection period. This process helped to minimize the inclusion of duplicate sites within the sample as they could be compared against existing saved content prior to data collection.

Every accessible page from each vendor's website was collected manually by the researchers and saved as HTML files for analysis, including vendors' homepages, product advertisements, and pages containing information related to the overall sales process (e.g., FAQ pages, customer feedback pages, shipping, and payment details). All text and images were then read and coded by hand using a qualitative case study design to assess the practices of both vendors and their customers (see also Aldridge & Askew, 2017; Copeland et al., 2020; Holt & Lee, 2022b). The contents were then subject to open coding to identify common themes across the data and their fit within the crime script process as identified by Cornish (1994). To that end, the researchers attempted to identify the processes distinct to each phase of a scene with specific emphasis on the actualization, doing, and exiting from the offense. In particular, the researchers attempted to identify vendors' statements regarding the processes of purchasing and delivery, as well as any possible steps occurring after receipt of goods to understand the procedures and phases involved. Content was also examined for descriptive information revealing motivations and conditions that may influence buyer and seller behavior. Additionally, the researchers attempted to identify conditional aspects of each process, which may stem from individuals' actions in a prior phase (Holt & Lee, 2022a; Hutchings & Holt, 2015).

Only publicly accessible data were examined in the current study. Specifically, the researchers created accounts with vendor sites in order to view content, particularly in the case of cryptomarkets. The researchers utilized false names and provided no identifiable information in order to engage in covert observation and did not post or engage with any vendor or market participant. No private or direct messages were included in this analysis as well. In this respect, the researchers engaged in passive observations so as to avoid affecting the discourse of the community in any way.

The current data provides a purposive sample of various online environments where individuals can acquire counterfeit currencies. It is also a convenience sample in that it is only reflective of shops and cryptomarkets that the researchers could identify and access. As a result, the sample may not reflect the entirety of the online counterfeit currencies market and is temporally bounded to the period of data collection. Furthermore, this sample contains a relatively small number of vendors operating on the Open Web, which may limit its potential generalizability to all online environments.

Findings

This analysis focused on the Open and Dark Web scenes of the market for counterfeit currencies, as well as the offline scenes where possible given the

comments made by vendors and customers (see also Holt & Lee, 2022a; Hutchings & Holt, 2015). The observable scripts are the primary foci of this analysis, along with potential scripts identified based on conditions arising in the process of making purchases. The findings flow from the preconditions of potential customers to initiation and entry processes of the market, followed by vendor actualization and doing of completing transactions, ending with the exit scripts of both parties in a given transaction. Though pseudonyms are used for all participants and websites, participants' direct quotes are provided when possible, using the original spelling, grammar, and syntax of participant posts (see also Holt, 2013; Holt & Lee, 2022b).

Preconditions for Purchase

Four of the vendors advertising counterfeit currencies gave subtle explanations as to why individuals would be interested in both purchasing and using fraudulent money, focusing primarily on the benefits of acquiring counterfeit currencies to benefit one's financial state. For instance, Vendor 1 stated: "Take the opportunity now to finally become wealthy a person in order to pay up your tuition fees and still have some money to buy school stuffs, pay your loans, hospital bills, utility bills and all your bills." Similarly, Vendor 4 stated: "you are just living your dream when you have plenty of money and cash in your hand, due to which you enjoy your life to the fullest." Relatedly, Vendor 6 posted a somewhat subtle message indicating why individuals should acquire their services:

> We solve your every need of cash and make sure you never need to go to a capitalist bank for loans in your life. Our ultimate goal is to help the common man with enough cash to run his daily activities. It is than they get and the poor end up suffering. Have you ever seen a mother begging the streets just to get a $20 bill to buy some bread for her kids? We don't want this to ever happen. . .so you have an urgent need for cash, know you are in the right place.

Finally, several vendors noted where their currencies could be used, such as Vendor 6, who wrote:

> Where can you spend the money ?
>
> Mc donald's, shops, restaurants, supermarkets, petrol shops, game hall, atm, banks,shopping malls, game and attraction parks, electronic shops, taxi, metro and train station, used to pay bus and any transportation and can be

Production

Vendors provided varying degrees of information regarding the ways they produced counterfeit currencies. For instance, Vendor 6 noted:

> We are the best, unique and legit suppliers of high quality undetected Counterfeit Money for many countries around the globe using ingredients such as cotton fiber (80-99%) originally sourced from common white linen rag, wood fiber (1-3%), titanium white (2-3.5% by weight of the total wood fiber), polyamide epichlorohydrin (0.5-2% by weight of the total cotton fiber), aluminum chloride, polyamide epichlorohydrin, melamine formaldehyde resin, animal glue. . . They by pass the UV and the Iodine Pen test and thus they can be used in stores,local banks, casinos, ATM and money changers.

Similarly, Vendor 4 stated:

> every banknote that passes under their [the site operators'] hands has a unique serial number which is engraved with close-to-real holograms. They possess impressed and well-designed underlying substances for all types of currencies available in different denominations. Our security features of banknotes include Intaglio printing Watermarks thread see-through register special foil, special foil elements Iridescent stripe and shifting colors.

Vendor 6 also highlighted the security features of their products, indicating they used: "Intaglio printing, Watermarks, Security thread, See-through register, Special foil/special foil elements, Iridescent stripe / shifting colors." Additionally, Vendor 7 wrote: "Each time we produce a new note, it is always tested in the country it is for. If everything goes well, we put it for sale." Only one vendor (Vendor 11) noted the downsides to their method of producing counterfeit $20 bills, stating: "The infrared detector normally detect our notes. (Sometimes not) We use 10 different serial numbers so some are repeated (in each order)."

There was only one site that indicated they used a different process, which may not be legitimate. Specifically, Vendor 8 stated:

> This is 100% real USD Currency stolen from the FED before it could be shredded. You have absolutely no Risk. Every year billions of dollars are selected for disposal. No one tracks money that's supposed to be destroyed. The "[site operators']" team has "access" to an almost limitless supply of cash that is marked for disposal. We want to maintain access to our cash source and don't want to get caught so we offer Cash in exchange for Bitcoins. We mail this cash to whatever address you wish in exchange for your bitcoins. We do not accept any other form of payment.

Table 3. Distribution of Currency Type ($n = 243$).

Currency type	*N* of advertisements	Percentage	Average listed price in USD
AED (Emirati Dirham)	1	0.4	—
AUD (Australian Dollar)	26	10.7	$504.36
CAD (Canadian Dollar)	20	8.2	$318.79
CHF (Swiss Franc)	5	2.1	$1,363.76
CNY (Chinese Yuan)	20	8.2	$358.62
DNR (Denarius)	1	0.4	—
EUR (Euro)	58	23.9	$970.58
GBP (British Pound Sterling)	27	11.1	$1,580.20
INR (Indian Rupee)	2	0.8	—
MYR (Malaysian Ringgit)	2	0.8	—
NZD (New Zealand Dollar)	2	0.8	—
QAR (Qatari Riyal)	1	0.4	—
SAR (Saudi Arabian Riyal)	1	0.4	—
THB (Thai Bhat)	2	0.8	—
TRY (Turkish Lira)	1	0.4	—
USD (United States Dollar)	62	25.5	$953.11
Unknown/unspecified	12	4.9	$345.83
Total	243	100	$861.99

Note. Not all product advertisements provided a cost price in their product description. As a result, the mean advertised price in USD was unattainable for several products/currency types.

Product Pricing

A total of 17 currencies were offered within the sample of counterfeit currency vendors (see Table 3), comprised of mostly Western currencies such as the U.S. Dollar (25.5%), Euro (23.9%), British Pound Sterling (11.1%), Australian Dollar (10.7%), and Canadian Dollar (8.2%). Non-Western currencies were also advertised by vendors, consisting mostly of Middle Eastern or Asian nations (see Table 3 for details).

The mean advertised price for all counterfeit currency products within the sample ($n = 243$) was $861.99 USD, with counterfeit U.S. Dollar products averaging $953.11 USD. British Pound Sterling had the highest average listed price at $1,580.20 USD, while counterfeit Canadian currency had the lowest average listed price at $318.79 USD (see Table 3 for details). It is worth noting that Middle Eastern and Asian currency products were frequently advertised without a price in their product description. As a result, the mean advertised price for many of these products/currency types were unattainable.

Additionally, two vendors noted that their pricing was dependent on the size of the order. For instance, Vendor 9 stated: "FOR ORDER OF FAKE USD BANK NOTES OF 10000 USD-49000 USD (COMMISSION IS 10%) ABOVE 50000 USD BULK ORDER OUR COMMISSION IS 5%." Vendor 7 stated: "Price rate is usually at 10% the required amount (shipping and handling fee included)." Similarly, Vendor 4 noted: "GENERALLY, WE CHARGE 10% THE AMOUNT YOU ARE ORDERING. *OUR MINIMUM ORDER IS GENERALLY $5000 FOR $500*."

Purchase and Delivery

In order to engage in a purchase, vendors require customers to contact them in some way. Open Web vendors tended to have multiple points of contact by comparison to those advertising on the Dark Web. For instance, Vendor 4 stated: "*Contact us to order any currency. To contact you can send us a message on live chat or Whatsapp*" By contrast, Dark Web vendors preferred some form of encrypted email (e.g., proton mail), such as Vendor 9, who indicated to customers: "Send Your shipping ad[d]ress and order quantity in Usd(minimum order 10,000 fake usd)."

Once the customer places their order, they would then send payment to the vendor, which would formally initiate the transaction. Payments were primarily made using cryptocurrencies, though bitcoin was most frequently used. For instance, Vendor 9 noted:

> We accept payment by bitcoin manually. When we get your odrer confirmation by mail, we will send you payment details by mail.After that you will make payment
>
> on our given bitcoin adress and also share with us Exact transcation id and all transaction screenshot by mail. After verifying your payment status, we will send courier to your given adress.

In much the same way, Vendor 7 wrote: "our method of delivery will be very safe and secured (Home Delivery).The notes will be printed and ship over to your provided location after you make the payment." Vendors who accepted other payment forms would specify their process, as with Vendor 4 who stated:

> OUR MOST PRIORITISED PAYMENT METHOD IS CRYPTO (BITCOINS, BITCOIN CASH, AND OTHERS), BUT WE ACCEPT OTHER PAYMENT METHODS IN VERY EXCEPTIONAL CASES (CASH APP, VENMO, WESTERN UNION, MONEYGRAM).

Three vendors indicated they were willing to take escrow payments, all of which were Dark Web vendors. While these sellers accepted the same payment method, they differed in their explanations of the process, as with Vendor 8 who stated:

> Escrow means the money (Bitcoin) is NOT going directly to the seller (us) but is being held by an impartial third party (Escrow Company) until you receive the goods and are happy with them. If there are any problems you can get your bitcoin back. . . We only use escrow on large orders because that escrow can delay payment for a long time and sometimes we lose our payment due to fraudulent buyers.

Vendors provided some clarity on their delivery methods to explain the security measures they take to evade detection and lower the risk customers may face from their purchase. For instance, Vendor 10 stated: "We do ship worldwide, though the regulation and implementation in respect to some of the products we sell often vary from country to country. We therefore advise you to make inquiries about the regulations that affect your region." Similarly, Vendor 11 stated: "We ship in an envelope as a payment for a product. . . If the package is inspected, they will see a paper with a fake invoice for payment for a computer or similar." Vendor 7 wrote: "Orders will be packaged with a serial seal to make sure that the banknotes are protected from damage, leakage, loss or inspection by airport authorities. Very safe and secure for the deliverance of your order." Some vendors also indicated they would provide tracking numbers for shipping, such as Vendor 1 who wrote:

> All orders are traceable on our mailing website to better ensure discreetness and comfort of the customer. When we send out your order, we'll email you the tracking reference number to track the location and Time or Day of delivery of package.

One vendor (Vendor 8) also noted a useful step in the process of purchasing counterfeit goods, stating:

> Most people use their home address and a fake first OR last name. Please do not tell us how the name and address are attached to you. You can also use ship to an abandoned house, a hotel, a PO box or wherever else you want it. We can not FEDEX a package to a PO box. Before mailing the package we confirm that the address is valid.

Shipping costs varied depending on multiple factors, including country of destination, specific carrier, speed of delivery, and product dimensions

(e.g., weight and height of shipment). Some vendors indicated they had a flat rate for shipping, such as Vendor 12, who wrote: "We have a flat rate for delivery - $19.99 (14 EUR)." Others attributed their costs to the delivery service, such as Vendor 11, who stated:

> The national postal service (Laposte fr, USPS US, etc) is the safest way and are included in our price (Takes 7-15 business days). But if you want it faster we can use DHL or FEDEX (€90, €180 depending on destination).

Vendor 13 noted: "All shipping prices are based on weight, height, width and your location."

Three vendors also noted potential difficulties and vulnerabilities in the process of shipping an illegal product. For instance, Vendor 13 stated:

> Orders will usually ship within 72 hours, however please do not stress if your order has not shipped for 3-4 days (US,Europe). There are a number of reasons dispatch may be delayed. We will notify you of any delay and attend to each order as quickly as possible. Once shipped, your order will generally take 3-4 days to reach most countries.

Two vendors also provided information regarding the potential that a package might be interdicted while in transit. Vendor 11 stated:

> No refund possible or free reship, Sorry. You must understand that there is a risk of 5% and assumes the responsibility when order. However I can add 20 notes free on your next order and use anti-xray bags for more security. Remember: I take pictures of the packages and keep the shipping receipts in case of dispute with the escrow.

Vendor 10 also stated:

> [The site] can regrettably accept no responsibility for products intercepted or lost in transit if you place an order for a product to be sent to a country where it is illegal. If your order got lost somehow (which actually never occur) we will resend the order in a different stealthy packaged manner. Since we both will have access to the track and trace of the package we can determine what happened. If it appears to be impossible to get your order delivered we will refund the money.

Discussion and Conclusions

The current study demonstrated that the process of purchasing counterfeit currency in online markets is similar to that of other illicit goods sold online, including fraudulent identity documents (Holt & Lee, 2022a), stolen data

products (Ablon et al., 2014; Holt & Lampke, 2010; Holt, Smirnova, & Chua, 2016), firearms (Holt & Lee, 2022b), and illegal drugs (Décary-Hétu & Giommoni, 2017; Jardine, 2021). Prospective buyers must first locate and identify vendors advertising the specific counterfeit currencies they are seeking to purchase and initiate the transaction process by contacting vendors using their preferred communications platform (e.g., email and instant messaging platform), which is a similar market initiation process to that of other illicit online markets. There are myriad reasons as to why individuals would be interested in acquiring fraudulent funds, though vendors primarily emphasized the financial benefits associated with purchasing counterfeit currency (see also Holt & Lee, 2022a, 2022b). For instance, vendors stated that individuals could acquire the flexibility to pay off any outstanding bills or loans they may have, and generally fulfill one's dreams and aspirations. Since these explanations are derived from sellers, further research is needed to understand buyers' perspectives and understand their rationale for making these illicit purchases. Specifically, future research would benefit from conducting qualitative analyses with current and/or former buyers to explore their rationale for acquiring counterfeit currency products.

Detailed descriptions of how products are made and subsequently shipped also reflected existing research involving other online illicit markets offering physical goods (see Copeland et al., 2020; Holt & Lee, 2022a, 2022b; Paoli et al., 2017). For instance, counterfeit currency vendors provided detailed information on the methods and processes involved in creating their counterfeit currencies (e.g., digital printing, traditional offset printing, and intaglio printing) to assure customers of their items' quality, including the security measures that were taken to ensure products are capable of evading detection. Similar descriptions were provided by fraudulent identity document vendors to inform prospective customers of their products' quality and security (see Holt & Lee, 2022a). This finding suggests vendors are aware of the illegal nature of their products and rely on well-known strategies to avoid the risk of detection (Finlay & Francis, 2019; Prime & Solomon, 2010; United States Treasury, 2006).

Vendors' preference for payments via bitcoin and other cryptocurrencies also mirrored extant research on the broader dynamics and economic practices of the online illicit marketplace (see Aldridge & Askew, 2017; Copeland et al., 2020; Holt & Lee, 2022a, 2022b). Few vendors expressed a willingness to use escrow services, which are common in other illicit markets (see Holt et al., 2016). In addition, customers were required to pay for products in advance of the goods being shipped to the customer. The actualization of transactions only occurred once payment was transferred from the buyer to the seller. Though several vendors indicated how items were packaged and shipped to

customers, it is unclear whether these measures reflect vendors' true practices (see also Copeland et al., 2020; Holt & Lee, 2022a). For instance, vendors may not package their products with a serial seal to ensure notes are protected from damage despite claiming to do so within their online advertisements. As a result, there may be discrepancies between the practices communicated in online advertisements and vendors' true practices offline. Further research is needed to assess these conditions, including collaboration with law enforcement agencies, to understand vendors' physical distribution practices.

Taken as a whole, this study reinforces the serious economic threats posed by the commercial exchange of counterfeit currencies and highlights the ease with which they can be acquired due to advancements in digital technology and e-commerce tools (Ekblom & Tilley, 2000; Kruisbergen et al., 2019; Mann & Sutton, 1998). While various forms of counterfeit currency have been in circulation throughout modern history, advancements in printing technology have streamlined the process of producing counterfeit money (Finlay & Francis, 2019). In addition, the growth of online markets may have expanded the overall size of this product market by generating more avenues to purchase these items (Rudner, 2008; Tremblay et al., 1998). Thus, the Internet may be crucial to offenders by flattening access to the networks that facilitate offending in offline spaces (Kruisbergen et al., 2019). Furthermore, this study corroborates prior research noting the significant impact of technology in altering the behavioral practices involved in the commission of a crime (Clarke & Cornish, 1985; Ekblom & Tilley, 2000; Jardine, 2021; Mann & Sutton, 1998).

While the current sample presents a threat to the study's external validity (i.e., ungeneralizable to all online counterfeit currency markets), the current findings provide insight into how counterfeit currencies are exchanged (e.g., advertised, acquired) on several online shops and forums. For instance, understanding the common procedures that buyers and sellers take to complete an economic transaction can help law enforcement agencies develop effective strategies aimed at disrupting the online counterfeit currency marketplace. Specifically, implementing strategies that target prominent market facilitators, such as widely used payment processors (e.g., cryptocurrency) and communications platforms (e.g., email servers), could generate a massive disruption in the market without arresting individual offenders (Van Der Zee, 2021). Targeting these established and accepted platforms could impact the overall ways in which market participants engage in commerce, including the sale and distribution of product (Holt, Smirnova, & Hutchings, 2016; Van Der Zee, 2021). Additionally, law enforcement agencies can flood the counterfeit currency marketplace with fake shops and convincing seller profiles to complicate buyers' identification of trustworthy sellers (Tzanetakis et al., 2016). This strategy would increase the complexity of decision-making among market

participants as identifying reliable sellers/buyers from undercover agents could cause both buyers and sellers to leave the market place due to the increased risk and difficulties in offending (Hutchings & Holt, 2017; Tzanetakis et al., 2016).

Despite the study's contributions to the extant literature, there are several limitations that must be considered. For one, this sample is derived largely from vendors operating on the Dark Web, which limits the generalizability of these findings to Open Web operations. In addition, the current sample may not reflect the practices of invitation-only vendors operating in closed or restricted online markets that are hidden from the public (see Holt & Dupont, 2019). These vendors may have their own unique practices that are distinct from the way other markets' function. Additionally, it is difficult to know vendors' true operational practices as the process of ordering, price negotiation, and delivery occur in private and away from public sight (Copeland et al., 2020; Holt, Smirnova, & Hutchings, 2016; Smirnova & Holt, 2017). Specifically, there may be discrepancies between the practices communicated in online advertisements and vendors' true practices offline. Future research would benefit from examining the accuracy of these online advertisements relative to offline practices.

The current study also focused primarily on shops, or single-operator websites, whose practices may be different from those of cryptomarkets or forums (Aldridge & Askew, 2017; Smirnova & Holt, 2017). Further study is needed with a broader sample of vendors from across the Open and Dark Web to determine the overall scope of the online counterfeit currency marketplace. Relatedly, it is possible that some vendors may have been undercover law enforcement agents posing as legitimate sellers to arrest potential buyers as part of sting operations (Aldridge & Askew, 2017; Holt, 2013; Holt & Lee, 2022b; Hutchings & Holt, 2015). Future research is needed to better assess the practices of online counterfeit currency vendors and their customers to understand the legitimacy of any claims made, as well as any changes in the process of acquiring fraudulent funds over time.

Appendix

Search Terms and Example Combinations Used for Site IdentificationFake euro dollars buy shop
Fake currency buy sell shop
Counterfeit currency buy shop
Counterfeit euro sell shop
Counterfeit dollar sell shop
Fake market Australian dollar shop
COUNTERFEIT buy Australian dollar shop

Dollar euro replica shop
Fake USD sell shop
Counterfeit USD buy

Declaration of Conflicting Interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: 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.

ORCID iDs

Thomas J. Holt https://orcid.org/0000-0002-5894-0172

Jin R. Lee https://orcid.org/0000-0003-1193-184X

References

Ablon, L., Libicki, M. C., & Golay, A. A. (2014). *Markets for cybercrime tools and stolen data: Hackers' bazaar*. Rand Corporation.

Aldridge, J., & Askew, R. (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*, 101–109.

Aldridge, J., & Décary-Hétu, D. (2016). Hidden wholesale: The drug diffusing capacity of online drug cryptomarkets. *International Journal of Drug Policy*, *35*, 7–15.

Barratt, M. J., & Aldridge, J. (2016). Everything you always wanted to know about drug cryptomarkets* (* but were afraid to ask). *International Journal of Drug Policy*, *35*, 1–6.

Borrion, H. (2013). Quality assurance in crime scripting. *Crime Science*, *2*(1), 6.

Brayley, H., Cockbain, E., & Laycock, G. (2011). The value of crime scripting: Deconstructing internal child sex trafficking. *Policing: A Journal of Policy and Practice*, *5*(2), 132–143.

Chase, A. (2019). *Feds counterfeiting experts fight flow of fake money*. Federal Reserve of Boston. https://www.bostonfed.org/news-and-events/news/2019/10/counterfeiting-experts-at-boston-fed-fight-flow-of-fake-money.aspx

Chiu, Y. N., Leclerc, B., & Townsley, M. (2011). Crime script analysis of drug manufacturing in clandestine laboratories: Implications for prevention. *The British Journal of Criminology*, *51*(2), 355–374.

Clarke, R. V. (1997). *Situational crime prevention: Successful case studies* (2nd ed). Harrow and Heston.

Clarke, R. V., & Cornish, D. B. (1985). Modeling offenders' decisions: A framework for research and policy. *Crime and Justice*, *6*, 147–185.

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review*, *44*(4), 588–608.

Copeland, C., Wallin, M., & Holt, T. J. (2020). Assessing the practices and products of Darkweb Firearm vendors. *Deviant Behavior*, *41*(8), 949–968.

Cornish, D. (1994). The procedural analysis of offending and its relevance for situational prevention. *Crime Prevention Studies*, *3*, 151—96.

Décary-Hétu, D., & Giommoni, L. (2017). Do police crackdowns disrupt drug cryptomarkets? A longitudinal analysis of the effects of Operation Onymous. *Crime, Law and Social Change*, *67*(1), 55–75.

Décary-Hétu, D., Paquet-Clouston, M., & Aldridge, J. (2016). Going international? Risk taking by cryptomarket drug vendors. *International Journal of Drug Policy*, *35*, 69–76.

Ekblom, P. (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*(4), 249–265.

Ekblom, P., & Tilley, N. (2000). Going equipped. *British Journal of Criminology*, *40*(3), 376–398.

Europol. (n.d.). Euro Counterfeiting. Retrieved August 4, 2022 from https://www.europol.europa.eu/crime-areas-and-statistics/crime-areas/forgery-of-money-and-means-of-payment/euro-counterfeiting

Finlay, R., & Francis, A. (2019). A brief history of currency counterfeiting. *RBA Bulletin*, *September*.

Flamand, C., & Décary-Hétu, D. (2019). The open and dark web. *The Human Factor of Cybercrime*.

Holley, P. (2016). They make the finest counterfeit money in the world. The US just recovered $30 million worth. *Washington Post*, November 22, 2016. https://www.washingtonpost.com/news/post-nation/wp/2016/11/22/they-make-fake-money-worth-more-than-cocaine-the-u-s-just-recovered-30-million-of-it/

Holt, T. J. (2013). Examining the forces shaping cybercrime markets online. *Social Science Computer Review*, *31/2*: 165–177.

Holt, T. J., & Bossler, A. (2016). *Cybercrime in progress: Theory and prevention of technology-enabled offenses*. Routledge.

Holt, T. J., & Dupont, B. (2019). Exploring the factors associated with rejection from a closed cybercrime community. *International Journal of Offender Therapy and Comparative Criminology*, *63*(8), 1127–1147.

Holt, T. J., & Lampke, E. (2010). Exploring stolen data markets online: Products and market forces. *Criminal Justice Studies*, *23*(1), 33–50.

Holt, T. J., & Lee, J. R. (2022a). A crime script analysis of counterfeit identity document procurement online. *Deviant Behavior*, *43*(3), 285–302.

Holt, T. J., & Lee, J. R. (2022b). A crime script model of Dark web Firearms Purchasing. *American Journal of Criminal Justice*. Advance online publication. https://doi.org/10.1007/s12103-022-09675-8

Holt, T. J., Smirnova, O., & Chua, Y. T. (2016). Exploring and estimating the revenues and profits of participants in stolen data markets. *Deviant Behavior*, *37*(4), 353–367.

Holt, T. J., Smirnova, O., & Hutchings, A. (2016). Examining signals of trust in criminal markets online. *Journal of Cybersecurity*, *2*(2), 137–145.

Hutchings, A., & Holt, T. J. (2015). A crime script analysis of the online stolen data market. *British Journal of Criminology*, *55*(3), 596–614.

Hutchings, A., & Holt, T. J. (2017). The online stolen data market: disruption and intervention approaches. *Global Crime*, *18*(1), 11–30.

Jardine, E. (2021). Policing the cybercrime script of darknet drug markets: Methods of effective law enforcement intervention. *American Journal of Criminal Justice*, *46*(6), 980–1005.

Judson, R., & Porter, R. (2010). *Estimating the volume of counterfeit U.S. currency in circulation worldwide: Data and extrapolation*. Federal Reserve Bank of Chicago Financial Markets Group. Policy Discussion Paper Series 2010-2.

Kennedy, J. P., Haberman, C. P., & Wilson, J. M. (2018). Occupational pharmaceutical counterfeiting schemes: A crime scripts analysis. *Victims & Offenders*, *13*(2), 196–214.

Klein, R. M., Gadbois, S., & Christie, J. J. (2004). *Perception and detection of counterfeit currency in Canada: note quality, training, and security features*. Proc. SPIE 5310, Optical Security and Counterfeit Deterrence Techniques V.

Kruisbergen, E. W., Leukfeldt, E. R., Kleemans, E. R., & Roks, R. A. (2019). Money talks money laundering choices of organized crime offenders in a digital age. *Journal of Crime and Justice*, *42*(5), 569–581.

Lavorgna, A. (2015). The online trade in counterfeit pharmaceuticals: New criminal opportunities, trends and challenges. *European Journal of Criminology*, *12*(2), 226–241.

Lee, J. R. (2021). *Understanding signals within the online stolen data market: An examination of vendors' signaling behaviors relative to stolen data price points*. Michigan State University.

Lee, J. R., Holt, T. J., & Smirnova, O. (2022). An assessment of the state of firearm sales on the Dark Web. *Journal of Crime and Justice*. Advance online publication. https://doi.org/10.1080/0735648X.2022.2058062

Liggett, R., Lee, J. R., Roddy, A. L., & Wallin, M. A. (2020). The dark web as a platform for crime: An exploration of illicit drug, firearm, CSAM, and cybercrime markets. In T. J. Holt & A. M. Bossler (Eds.) *The Palgrave handbook of international cybercrime and cyberdeviance* (pp. 91–116). Springer.

Mann, D., & Sutton, M. (1998). NETCRIME: more change in the organization of thieving. *The British Journal of Criminology*, *38*(2), 201–229.

Martinez, J. A., Rutledge, P. C., & Sher, K. J. (2007). Fake ID ownership and heavy drinking in underage college students: prospective findings. *Psychology of Addictive Behaviors*, *21*(2), 226.

Martinez, J. A., & Sher, K. J. (2010). Methods of "fake ID" obtainment and use in underage college students. *Addictive Behaviors*, *35*(7), 738–740.

Meland, P. H., Bayoumy, Y. F. F., & Sindre, G. (2020). The Ransomware-as-a-Service economy within the darknet. *Computers & Security*, *92*, 101762.

Morselli, C., & Roy, J. (2008). Brokerage qualifications in ringing operations. *Criminology*, *46*(1), 71–98.

Musco, S., & Coralluzzo, V. (2016). Sneaking under cover: Assessing the relevance of passports for intelligence operations. *International Journal of Intelligence and Counter Intelligence*, *29*(3), 427–446.

Paoli, G. P., Aldridge, J., Nathan, R., & Warnes, R. (2017). *Behind the curtain: The illicit trade of firearms, explosives and ammunition on the dark web*. Rand Corporation.

Perez, M. E., Castaño, R., & Quintanilla, C. (2010). Constructing identity through the consumption of counterfeit luxury goods. *Qualitative Market Research: An International Journal*, *13*(3), 219–235.

Prime, E. L., & Solomon, D. H. (2010). Australia's plastic banknotes: Fighting counterfeit currency. *Angewandte Chemie International Edition*, *49*(22), 3726–3736.

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

Smirnova, O., & Holt, T. J. (2017). Examining the geographic distribution of victim nations in stolen data markets. *American Behavioral Scientist*, *61*(11), 1403–1426.

Tompson, L., & Chainey, S. (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.

Tremblay, P., Cusson, M., & Morselli, C. (1998). Market offenses and limits to growth. *Crime, Law and Social Change*, *29*(4), 311–330

Tzanetakis, M., Kamphausen, G., Werse, B., & von Laufenberg, R. (2016). The transparency paradox. Building trust, resolving disputes and optimising logistics on conventional and online drugs markets. *International Journal of Drug Policy*, *35*, 58–68.

United States Treasury. (2006). *The use and counterfeiting of United States currency abroad, Part 3*. Author. https://www.treasury.gov/about/organizational-structure/offices/DomesticFinance/Documents/the%20use%20and%20counterfeiting%20of%20u.s.%20currency%20abroad%20%20part%203%20september2006.pdf

Van Der Zee, S. (2021). Shifting the blame? Investigation of user compliance with digital payment regulations. In M. Weulen Kranenbarg & R. Leukfeldt (Eds.) *Cybercrime in context* (pp. 61–78). Springer.

Wright, R., & Decker, S. H. (1994). *Burglars on the job: Streetlife and residential break-ins*. Northeastern University Press.

Wright, R., & Decker, S. H. (1997). *Armed Robbers in action: Stickups and street culture*. U. S. Department of Justice.

Author Biographies

Thomas J. Holt is a Professor in the School of Criminal Justice at Michigan State University. 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 R. Lee is an Assistant Professor in the Department of Criminology, Law and Society at George Mason University. His research interests are in cybercrime, online interpersonal violence, cybersecurity, cyberpsychology, computer-mediated communications, and big data.

Elizabeth O'Dell is a Master's Student in the School of Criminal Justice at Michigan State University, with an interest in cybercrime, counterfeiting, and online research methods.