International Journal of Cybersecurity Intelligence & Cybercrime

Volume 5 | Issue 2 Article 2

8-22-2022

Dynamics of Dark Web Financial Marketplaces: An Exploratory Study of Underground Fraud and Scam Business

Dark Web, Cryptocurrency, Dark Web Financial Marketplace, Fraud, Scam

Jung et al. (2022). *International Journal of Cybersecurity Intelligence and Cybercrime, 5*(2), 4-24.

Dynamics of Dark Web Financial Marketplaces: An Exploratory Study of Underground Fraud and Scam Business

Bo Ra Jung*, Boston University, U.S.A.
Kyung-Shick Choi, Boston University, U.S.A.
Claire Seungeun Lee, University of Massachusetts Lowell, U.S.A.

Keywords: Dark Web, Cryptocurrency, Dark Web Financial Marketplace, Fraud, Scam, Consumer Safety Program, Routine Activity Theory

Abstract:
The number of Dark Web financial marketplaces where Dark Web users and sellers actively trade illegal goods and services anonymously has been growing exponentially in recent years. The Dark Web has expanded illegal activities via selling various illicit products, from hacked credit cards to stolen crypto accounts. This study aims to delineate the characteristics of the Dark Web financial market and its scams. Data were derived from leading Dark Web financial websites, including Hidden Wiki, Onion List, and Dark Web Wiki, using Dark Web search engines. The study combines statistical analysis with thematic analysis of Dark Web content. Offering promotions and customer services with the payment methods of cryptocurrencies were prevalent, similar to the Surface Web's e-commerce market. The findings suggest that the Dark Web financial market is likely to harbor scams targeting Dark Web buyers. Dark Web sellers construct a website to sell scam products and recommend purchasing Escrow services to ensure safe transactions as an additional scam. The results from this study provided empirical support for the components of the routine activity theory of the Dark Web financial market to substantiate a more comprehensive view of patterns of fraud/ scams. Enhancing law enforcement capabilities of investigating financial marketplaces and promoting public awareness and consumer safety programs are discussed as effective preventive measures.

Introduction

The Dark Web refers to a secretly encrypted communication system that can only be accessed via unique browsers (Mirea et al., 2019). The Surface Web is the part of the Internet in which only 4% of the indexed content is available via search engines Google or Bing (Chikada & Gupta, 2017). The rest of the content can be discovered on the Deep Web. The Onion Router (Tor) network is one of the most popular web browsers to search the Deep Web continent. It protects the user identity, by allowing them to remain anonymous when visiting online sites ending with ". onion" (Yetter, 2015). Tor also supports website publishers in generating websites without providing legal publisher information (Ahvanooey et al., 2021). With minimal risk of identity disclosure, Tor has become a platform for cybercriminals to engage in illegal activities in the cyber realm.

The Dark Web market is an e-commerce platform within the Dark Web in which buyers and sellers trade a wide range of illicit goods and services such as drugs, child pornography, stolen identities, money

*Corresponding author
Bo Ra Jung*, Department of Criminal Justice, Boston University, 1010 Commonwealth Ave, 5th floor, Boston, MA, 02215, U.S.A.
Email: bzj2@bu.edu

laundering services, and others (Aldridge & Decary-Hétu, 2015; Aldridge & Décary-Hétu, 2016; Martin, 2014; Rudesill et al., 2015). The main categories of the Dark Web financial market products include fake credit cards, bank accounts, wire transfers, counterfeit, and crypto-related services—also identified as financial services. The Dark Web market is similar to conventional online markets on the Surface Web like eBay or Amazon. However, it evades government regulations or sanctions under decentralized peer-to-peer anonymous networks (Barratt, 2012; Nardo, 2011).

The arrival of the online Dark Web market has created an active online criminal marketplace that offers high financial rewards to criminals selling cloned credit cards generated from phishing, vishing, smishing, pharming, and cryptocurrency scams (Weber & Kruisbergen, 2019). According to the recent Internet Crime Complaint report (Internet Crime Complaint Center, 2022), monetary losses from credit card fraud and internet scams, including phishing, vishing, smishing, and pharming, were $172,998,385 and $44,213,707, respectively. Monetary losses from cryptocurrency-related frauds were $246,212,432. The total monetary loss from these financial cybercrimes was estimated at $463,424,524. Furthermore, an exponential increase in financial losses was observed, with an increase of $1.6 billion within a year based on cryptocurrency-related cybercrime. Financial cybercrime losses are estimated to reach approximately $10.5 trillion by 2025, with expected growth of 15% yearly.

Cryptocurrencies (e.g., Bitcoin, Monero, and Ethereum) are anonymized payment transaction systems based on blockchain technology that allows the Dark Web market to record and secure every transaction (Wątorek et al., 2021). Most cryptocurrencies offer currency exchange, exceedingly low transaction fees, instant bank transactions, and other convenient services that attract users (Choi, 2018; Wątorek et al., 2021). As the popularity of cryptocurrencies in the globalized online markets has increased over the past decade, the number of financial cybercrimes has increased exponentially (Nicholls et al., 2021). While global concern has been raised over the rate of financial cybercrimes, the global regulatory framework for cryptocurrencies continues to be limited, due to the anonymity afforded to cybercriminals, thereby hindering law enforcement investigations (Pieters & Vivanco, 2017). In the absence of guaranteed fairness, fraudulent schemes are prevalent in the Dark Web market and create a scam culture (Goldfeder et al., 2017).

In demand for buyer protection, an authorized third-party called “Escrow” has been added to the Dark Web market. This system regulates the money transfer, holding the payment until the buyer confirms delivery of the right product. If the buyer does not receive the product, the escrow service intervenes and processes refunds (Goldfeder et al., 2017). While escrow has been widely used for fair payment transactions (i.e., the Silk Road case; Christin, 2013), escrow failed to provide sufficient protection for the Dark Web market for fraudulent escrow services (Anderson et al., 2013; Drew & Moore, 2014).

While many studies are addressing the damages from financial cybercrime, few studies have focused on the issues of illegal financial marketplaces on the Dark Web. Financial cybercrime investigations have encountered limited digital evidence to investigate anonymous Dark Web security. This study aims to contribute to the criminology literature based on Cohen and Felson’s routine activity theory (Cohen & Felson, 1979) to understand the criminals’ motivational factors, challenges of criminal justice responses, and criminal operations of the Dark Web financial services. Primarily, the study focuses on examining target suitability components to uncover (1) what main products scammers encourage customers to purchase, (2) how financial market vendors operate their business, and (3) which marketing strategies are used to scam

potential buyers in the Dark Web financial market. This inquiry will begin with a review of the relevant literature on routine activity theory concerning scams in the Dark Web market. A discussion of research methods and findings will follow the theoretical framework section. A summary of this study's key findings and its potential policy implications will be addressed in the conclusion.

Theoretical Framework: Routine Activity Theory

Routine activity theory offers a theoretical framework to understand how criminals decide to commit certain crimes. In 1979, Cohen and Felson proposed their routine activity theory, which focused mainly on opportunities for criminal events. Cohen and Felson posited that three significant factors contribute to criminal victimization: (a) motivated offenders, (b) suitable targets, and (c) the absence of capable guardianship. Crime is likely to occur via the convergence of the three factors. A lack of any of the three would most likely result in the prevention of a crime occurrence.

Cyberspace shares a similar social environment with the physical world. Choi (Choi,2008; 2010; 2015; 2018) asserted that cyberspace is another dimension of real space closely correlated to the physical world and that online users also develop illegitimate subcultures within the realm of cyberspace. Cyberspace reflects the physical world's "socioeconomic and cultural dimensions" (Castells, 2002; Choi, 2018). As for how the routine activity theory is applied to the physical world, many cybercrime studies posit there are various criminal motivations required to commit cybercrimes. Like street criminals, "greed, lust, power, revenge, adventure, and the desire to taste *the forbidden fruit*" (Grabosky, 2000) are the most evident motivations of cybercriminals.

Cybercriminals who commit financial fraud (fraudulent sellers) are motivated by monetary gain. Verizon DBIR Report (Verizon, 2016) stated that "there was never any real danger of the financial motive losing its prominence, as even at its peak, espionage remained a far distant second" (p. 8). Individuals tend to make rational decisions based on the extent to which they expect "the choice to maximize their profits or benefits and minimize costs or losses" (Akers, 2013, p. 26). According to Broadhurst, criminals also acknowledge that they can make more money using technology, with low risks of getting caught and minor penalties even if they get caught (Broadhurst et al., 2013). It is a much "cleaner" way of profiting from crime because high profit and reduced probability of arrest drive criminals to switch from committing traditional crimes to engaging in cybercrimes (Ilievski & Bernik, 2016). Ultimately, this study assumes that cybercriminals who choose to commit fraudulent activities in the Dark Web market fully consider limited law enforcement capabilities and potential expansions of criminal activities – that is, they find these circumstances as paramount illegitimate opportunities to gain monetary success (Ahmadi & Yang, 2000; Onkvisit & Shaw, 1989).

To attract targets for financial fraud, offenders (fraudulent sellers) provide target attractiveness preferred by the targets. Referencing routine activity theory, the target attractiveness associated with financial fraud can be value, visibility, and accessibility (Cohen & Felson, 1979). To prove the vendor's value, offenders provide reputation, feedback, promotions, and consumer experiences that affect the targets' decision to engage with fraudulent sellers. In the event that a vendor's reputation or rating becomes diminished, it would most likely result in a reduction in their future income from fraudulent activities (Décary-Hétu et al., 2016). For visibility, offenders often advertise their products on Dark Web forums to attract their targets

(Nunes et al., 2016). Increasing visibility to the targets affects the number of targets accessing the vendor, which influences and can determine any monetary gains for an offender. Yar (2005) stated that accessibility in cyberspace is related to the structural aspects of online environments. Since fraudulent financial markets operate on the Dark Web, users with no boundaries can increase the number of targets accessing the vendors (Leukfeldt & Yar, 2016). Target attractiveness is essential when committing financial fraud on the Dark Web marketplace.

The Dark Web marketplace is becoming more organized and expanded with an increasing number of criminal activities and transactions (Ablon et al., 2014) via creating a safe criminal networking hub that offers relatively low risk of criminal penalties - in some cases being essentially non-existent (Koch, 2019). In terms of capable guardianship, the current capabilities of many law enforcement agencies are minimal despite a heightened level of awareness and concern for the role recent technology has in facilitating cybercrime and instances of online victimization. Reduced arrest probability with vailed identities energizes cybercriminals' engagement in Dark Web activity (Buxton & Bingham, 2015). The Dark Web market has offered a more comprehensive range of products and greater convenience than offline transactions (Barratt et al., 2014).

Cryptocurrency transactions are commonly used when purchasing and trading illegal goods and services in the Dark Web marketplace (Lee et al., 2019). According to Foley et al. (2019), Bitcoin transactions were related to illegal activities on the Dark Web. Predominantly, virtually untraceable financial transaction systems significantly facilitate new forms of online financial crime activities. Cryptocurrencies introduced a new form of money laundering using a crypto wallet and crypto mixer service (Schafer & Graham, 2002). Cybercriminals in the financial market perform their illegal activities by issuing anonymous debit cards or virtual credit cards from hacked identities used and sold in illegal transactions (Piazza, 2016).

Studies have examined the fraud scammer's behaviors and operations in the Dark Web markets. Fraud and scams on the Internet are 20 times higher than offline fraud scammers in non-digital marketplaces (Bajari & Hortaçsu, 2004; Snyder, 1999; Waters, 2003). This tenet is important to understand how scammers target their victims in Dark Web markets. The risks involved in purchasing from Dark Web markets are driven by the anonymity of seller information, unreliable guarantees, the lack of manufacturer warranties, and the unavailability of after-sale service (Aldridge & Décary-Hétu, 2016; Zhang et al., 2022). Scammers comply with their customers by eliciting compliance using the false promise of rewards and offering discounts (DeLiema et al., 2021; DeLiema & Witt, 2021) and imposing Escrow services in which a third party temporarily holds the money until the transaction is secured. Some marketplaces provide feedback ratings from buyers, number of orders history, number of transactions, and years of experience as an advertising method.; a valuable form of confirmation of trustworthiness for those offering their services on the Dark Web.

Compared to the Dark Web market, there has been much research on the convergence of motivated offenders and suitable targets in e-commerce market fraud on the Surface Web across various disciplines (Zhang et al., 2013; Zhang et al., 2022). Significant challenges exist when attempting to verify legitimate sellers and establish a fine reputation due to the consequences of fraud behaviors on e-commerce platforms. Trust fraud is widespread in which sellers falsely boost their reputations with fake reviews on e-commerce market platforms such as Taobao and eBay (Zhang et al., 2013; Zhang et al., 2022). Reputation manageme-

nt is a system that aims to avoid interaction with undesirable participants such as fraudulent sellers (Yu & Singh, 2000; 2002). Due to its reliability, a high feedback rating causes an estimated additional 10% of consumers to visit the vendor, which is closely tied to the profitability of a vendor. Sellers exchange products with extremely meager prices (as little as a penny), or sometimes offer items for free to receive positive feedback to falsely boosts their feedback rating and collect reviews as a "verified seller" (Brown & Morgan, 2006; Dini & Spagnolo, 2009; Zhang et al., 2013). False feedback systems are advantageous to scammers to attract more consumers to commit fraud against in the e-commerce market on the Surface Web.

Other studies explore why victims fall for online scams and discuss the operation of online market frauds on the Surface Web (Button et al., 2014; Lea et al., 2009). Whitty and Buchanan (Whitty & Buchanan, 2012) argue that authority and legitimacy are key triggers that make consumers can become victims of fraud. Online scammers perform crimes by assuming a professional or a legitimate facade. Scammers build fake websites that refer to well-known legitimate companies with sophisticated designs, stolen logos, the same transaction services, and similar domain names (Banday & Qadri, 2011). Fake websites are advertised to offer low prices and benefits on products to attract online consumers (Zhang et al., 2013). Victims of online market fraud often only realize that they have been defrauded when their goods or services do not arrive. The research provides an essential contribution to understanding how scammers commit online market fraud on the Surface Web, similar to scams on the Dark Web.

As previously addressed, this study is designed to facilitate an important role in understanding the trends and patterns of Dark Web market operations, focusing on the characteristics of Dark Web financial services, their products and services, and factors of harboring scams targeting the buyers. Furthermore, the study aims to build a bridge between criminological literature and cybercrime-related disciplines, thereby seeking to help both law enforcement agencies and the public better understand emerging Dark Web illegal operations.

Methodology

Since only a few studies focused on empirical reviews of the Dark Web financial marketplace characteristics (Elbahrawy et al., 2020), this study scrutinizes different types of Dark Web financial marketplaces. It compared each vendor to the different factors in Dark Web financial marketplaces correlated to its scam. In doing so, we combined a quantitative analysis (i.e., logistic regression) and qualitative analysis (i.e., thematic analysis). For the statistical analysis, utilizing IBM SPSS software, we conducted a logistic regression analysis to delineate the Dark Web financial marketplace pattern and determine the main factors that encourage consumers to associate with illegal trading of financial goods. Data were collected from December 2021 to January 2022, and coding and analysis were conducted in March 2022.

For qualitative analysis, we used thematic analysis, which is the process of identifying interesting and/or important patterns or themes (Maguire & Delahunt, 2017). The thematic analysis of the financial crime on the Dark Web market was conducted in a six-phase framework (Braun & Clarke, 2006; Clarke & Braun, 2013). The framework includes the following steps (Byrne, 2021): (1) Step 1: Become familiar with the data by carefully re-reading the entire dataset; (2) Step 2: Generate initial codes, which are "the fundamental building blocks of what will later become themes, (3) Step 3: Search for themes, (4) Step 4: Review themes, (5) Step 5: Define themes, and (6) Step 6: Write-up. In doing so, a computer-aided qualitative data analysis

software called NVivo was used to perform a systematic thematic analysis of financial services on the Dark Web. This software helps organize data, conduct a systematic analysis, code data into categories, and present data in an organized manner (Kaefer et al., 2015; Lee, 2021; Leech & Onwuegbuzie, 2011). These processes assist in systematizing and ensuring rigor in the research and analysis processes. In addition, the spreadsheet used to annotate the variables, codes, and information from each document is also fully documented in NVivo.

Sample and Procedure

Determining the accurate size to obtain a representative sample is one of the biggest challenges to conducting an empirical analysis of internet sites under Dark Web anonymity (Choi, 2018). The Tor network's continuous fluctuation of IP addresses, and the resilience of creating a cloned website with a different URL aggravates the actual size, dimensions, and composition of the Dark Web financial marketplace. Therefore, determining the actual size of the Dark Web market is difficult. Using representative sampling techniques in social science research is impossible without the actual population (Choi, 2018). As a result, studies that use websites as the unit of analysis frequently depend on a less accurate purposive sampling technique (Schafer & Graham, 2002).

This research utilizes quantitative data, a sample of 117 financial market sites and 31 Escrow sites collected on the Dark Web. The data for the present study were collected from Dark Web financial markets and Escrow sites listed on the main Dark Web forums: Hidden Wiki, Onion List, and Dark Web Wiki. The most well-known Dark Web browser, the Tor browser, was used to access and collect marketplace sites from Dark Web vendors. The Dark Web financial markets and Escrow services are generally able to access without registration to purchase illegal financial products. Under the Dark Web forums, the financial vendors required registration to access their services. The nature of the Dark Web that cybercriminals organize globally, few market websites inform that the region of the vendor is located in Europe, China, and Russia (Kadlecová, 2015). The international vendors in this research are English-speaking marketplaces that operate services and deliver physical products to the United States.

Property of Measures

Each site was examined to identify the information and variables that reveal its characteristics, the type of products, type of cryptocurrency, customer service, and security. Based on the information provided by the underground financial marketplace, a codebook was created, and the sample was coded independently according to the codebook. The years of experience were measured by years of experiences, and the other variables were dichotomized as 0=No and 1=Yes.

Table 1 shows the findings from the descriptive analyses of sample characteristics reflecting dependent measures, scam lists, and independent measures, target attractiveness, in the current study.

Dependent Variable

The scam lists. The scam list was measured as a binary scale variable coded as either "yes (1)" or "no (0)" to identify whether each of the sites is a scam site or not by reviewing scam reports. According to the data, the average number of vendors on the scam list was 0.63 (SD= 0.484). 63.2% (n=74) of the vendors reported associating selling fraudulent products to their customers in the Dark Web financial market.

Table 1. Descriptive Statistics (*N*=117)

Variables	Mean (SD)	*N* (%)
Dependent Variable		
Vendors on Scam List	0.63 (0.484)	74 (63.2%)
Independent Variables		
Target Attractiveness		
Duplicate Predominant Business	0.39 (0.991)	22 (18.8%)
Carding: Scam Products		
Prepaid Card	0.26 (0.439)	30 (25.6%)
Cloned Card	0.28 (0.452)	33 (28.2%)
Credit Card	0.20 (0.399)	23 (19.7%)
PayPal Account	0.15 (0.354)	17 (14.5%)
Gift Card	0.12 (0.326)	14 (12.0%)
Carding: Customer Service		
Brands (*N*=53)		
Visa	0.92 (0.267)	49 (41.9%)
Mastercard	0.79 (0.409)	42 (35.9%)
American Express	0.49 (0.505)	26 (22.2%)
Discover	0.09 (0.295)	5 (4.3%)
PIN Number (*N*=64)	0.97 (0.175)	62 (53.0%)
Personal Information (*N*=64)	0.17 (0.383)	11 (9.4%)
Wire Transfer: Scam Products		
Paypal	0.20 (0.399)	23 (19.7%)
Western Union	0.20 (0.399)	23 (19.7%)
Money Laundry: Scam Products		
Counterfeit	0.12 (0.328)	14 (12.0%)
Cryptocurrency	0.15 (0.354)	17 (14.5%)
Counterfeit: Customer Service (*N*=6)		
UV Test	1.00	6 (5.1%)
Cotton Base Paper	1.00	6 (5.1%)
General Customer Service		
Shipping and Delivery	0.98 (0.130)	115 (98.3%)
Return and Refund	0.53 (0.501)	62 (53.0%)
Payments Method		
Bitcoin	0.98 (0.130)	115 (98.3%)
Monero	0.53 (0.501)	62 (53.0%)
Discount	0.08 (0.269)	9 (7.7%)
Communication via Email		
Security and Privacy		
Years of Experience	5.11 (3.389)	73 (62.4%)

Variables	Mean (SD)	*N* (%)
Website Verification	0.42 (0.495)	73 (62.4%)
Hidden Wiki	0.23 (0.423)	49 (41.9%)
DeepDotWeb	0.10 (0.305)	27 (23.1%)
Tor Link	0.11 (0.316)	12 (10.3%)
Onion List	0.14 (0.345)	13 (11.1%)
Escrow	0.64 (0.482)	16 (13.7%)
Currency Exchange Service		
USD	0.97 (0.159)	114 (97.4%)
EUR	0.26 (0.443)	31 (26.5%)
GBR	0.13 (0.336)	15 (12.8%)
CAD	0.06 (0.238)	7 (6.0%)
Source of Products		
Skimming	0.11 (0.316)	13 (11.1%)
Hacking	0.16 (0.370)	19 (16.2%)

Note: Some variables may have multiple characteristics within a group.

Independent Variable

Scam products. The carding scam product was coded as either "yes (1)" or "no (0)" to measure the product availability on the each of the market sites: 28.2% (n=33) Cloned cards, 25.6% (n=30) Prepaid cards, 19.7% (n=23) Credit card, 14.5% (n=17) PayPal Account, and 12.0% (n=14) Gift Card. Four major types of card brands 1) Visa (92.4%, n=49), 2) Master (49.1%, n=42), 3) American Express (49.1%, n=26), and 4) Discover (9.4%, n=5) were observed as customer service that provides to choose card brands that customers prefer. PIN (96.9%, n=62) and personal information (9.2%, n=11), which contains the original card holder's information such as name, address, and social security numbers, were provided to the customer when purchasing carding products.

The wire transfer products, 19.2% (n=23) of PayPal and Western Union transfers were available, and the wire money laundry products, 12.2% (n=14) counterfeit, 14.5% (n=17) cryptocurrency-related services were also available. All vendors who sell counterfeit are observed to use cotton fiber and take UV test that produces high-quality counterfeit money. Cryptocurrency laundry contains services for crypto wallet, crypto mixer, and crypto exchange. A Crypto mixer is a software platform that makes a crypto wallet untraceable by randomizing coins when sent to the receiver.

Customer services. The carding scam product was coded as either "yes (1)" or "no (0)" to measure the product availability on the each of the market sites: 28.2% (n=33) Cloned cards, 25.6% (n=30) Prepaid cards, 19.7% (n=23) Credit card, 14.5% (n=17) PayPal Account, and 12.0% (n=14) Gift Card. Four major types of card brands 1) Visa (92.4%, n=49), 2) Master (49.1%, n=42), 3) American Express (49.1%, n=26), and 4) Discover (9.4%, n=5) were observed as customer service that provides to choose card brands that customers prefer. PIN (96.9%, n=62) and personal information (9.2%, n=11), which contains the original card holder's information such as name, address, and social security numbers, were provided to the customer when purchasing carding products.

Security and privacy. The measure of security and privacy, the average years of experience in the financial market was observed for 5.11 (SD= 3.389) years. 41.9% (n=49) of websites verified by famous Dark Web forums prove the safety and trust of the vendor. Website verification consists of 5 resource items. Hidden Wiki (23.1%, n=27), Onion List (13.7%, n=16), Tor Link (11.1%, n=13), DeepDotWeb (10.3%, n=12) were coded as either "yes (1)" or "no". In addition, Escrow service (11.1%, n=13) and third-party mediate service for secure transactions were observed for security and privacy options.

Currency exchange service. In terms of currency exchange services, eight currency exchange services were observed on specific sites. Mainly, 97.4% (n=114) USD, 26.5% (n=31) EUR, 12.8% (n=15) GBP, and 6.0% (n=7) CAD were found.

Source of products. Two main sources of products were identified and coded as either "yes (1)" or "no (0)" 16.2% (n=19) hacking and 11.1% (n=13) skimming were observed when vendors revealed the source of the product.

Results

Target Attractiveness on Scam Lists

Table 2 shows the logistic regression analysis of target attractiveness measures vendors on scam lists. The results indicated that the vendors with duplicate domains were correlated with a significant increase in the chance of being a scamming site by approximately 4.6 times (b = 1.53 and Odds Ratio = 4.61 with p <.05). The variable selling cloned cards was correlated with a reduction in the chance of being a scamming site at approximately 97% (b = -3.54 and Odds Ratio = .03 with p <.05). PayPal transfer product was highly correlated with Dark Web scamming sites by more than 31times (b = 3.46 and Odds Ratio = 31.88 with p <.05).

The Monero payment method dramatically increased the likelihood of a scamming site by approximately 242 times (b = 5.49 and Odds Ratio = 241.97 with p <.05). This result may indicate that Monero is a substantially attractive payment method to cybercriminals. Since the Colonial Pipeline hackers using a bitcoin transaction, which stores all token transactions in its history and is visible to everyone, were successfully traced by the FBI, Monero is increasingly the cryptocurrency of choice among cybercriminals because Monero has additional anonymity built into the payment transaction (Sigalos, 2021).

In addition, the Hidden Wiki Verification service was correlated with an increase in the likelihood of a scamming site by more than 17 times (b = 2.86 and Odds Ratio = 17.52 with p <.05). Email communication service offered from the site was correlated with about 92% decrease in the likelihood of scamming sites with a borderline significance (b = -2.5 and Odds Ratio = .08 with p =.057).

Thematic Analysis Results

In the quantitative data analysis, we identified key variables associated with vendor scams, namely (1) payment method (Monero); (2) type of product (cloned cards, PayPal); and (3) verification method (Hidden Wiki and email). In the thematic analysis, similar themes emerged. A prevalent trend was the use of cryptocurrencies as payment methods, similar to the operation of the e-commerce market on the Surface Web.

Table 2. Logistic regression of predicting Dark Web scam site

	Dark Web Scam Site		
	B	SE	Exp(B)
Target Attractiveness			
Duplicate Domains	1.53	.75	4.61*
Years of Experience	.18	.14	1.20
Hacking Source of the Funds	-2.27	1.33	.10
Cloned Cards Products	-3.54	1.46	.03*
PayPal Transfer Products	3.46	1.56	31.88*
Cryptocurrency Laundry Products	-1.93	1.58	.145
Monero Payment	5.49	1.69	241.97**
Escrow Payment	-.97	1.25	.38
Hidden Wiki Verification	2.86	1.26	17.52*
Communication Email	-2.50	1.32	.08
Nagelkerke's R^2		.81	

*$p < .05$, **$p < .01$

The findings show that Dark Web financial markets likely harbor scams targeting Dark Web buyers. Scam retailers on the Dark Web create websites and recommend using Escrow services to ensure transaction safety. Payment card fraud refers to the acquisition and unauthorized use of payment card data, such as credit card numbers, billing addresses, security codes, and expiration dates (Lusthaus, 2020). In this study, payment card fraud occurs when market vendors sell credit and debit cards. Vendors advertise many of these products as legitimate; however, at least some of the advertised products are scams. In the thematic analysis, we demonstrate how the emerging three themes—cryptocurrency, pricing, and customer trust—shape Dark Web financial markets and enable the identification of potential victims.

Payment

Cryptocurrencies are virtual assets supported by large networks of computers (Lusthaus, 2020). Bitcoin is the most commonly used payment method on Dark Web markets, followed by Monero (Lusthaus, 2020). It is also possible to purchase Monero from some exchanges but not all: for example, the primary cryptocurrency exchange Coinbase does not support this currency. Coinbase offered 30 different cryptocurrencies for trading in 2020, but Monero was not one of them due to its enhanced nature of anonymity, which has been disliked by US regulators. This, on the other hand, indicates that Monero is expected to gain popularity on Dark Web marketplaces because it provides anonymity by default (Lusthaus, 2020).

The former underground marketplace Alpha Bay positioned Monero as a more secure alternative to Bitcoin (Georgoulias et al., 2021; Soska & Christin, 2015). The findings in Table 2 demonstrate that websites that accept Monero are likely to sell scam products. As mentioned earlier, one of the largest cryptocurrency exchange platforms, Coinbase, does not support Monero. Bitcoin is the default payment method, although some vendors offer Monero as an optional alternative.

KryptoPayPal, one of the most gripping financial services used Monero in our dataset, was active on November 12, 2021. The vendor includes a memo on the site: "Q: OK, is this a scam? A: That is up to you to

decide. If you believe it is, then it is best that you pursue other financial opportunities." The vendor (KryptoPaypal) advertises that Hidden Wiki has verified the site, but it was revealed to be a scam. KryptoPayPal advertises PayPal accounts obtained via hacking for sale. In other words, potential customers purchase illegitimate PayPal accounts (a characteristic of the Dark Web marketplace).

As presented in Table 2, the findings indicate that the offering of Escrow services is negatively correlated with the likelihood that a website sells scam products. Although it was not a significant result, Escrow services appear to be an important service in the Dark Web financial marketplaces.

Figure 1-4 Dark Web Financial Vendors

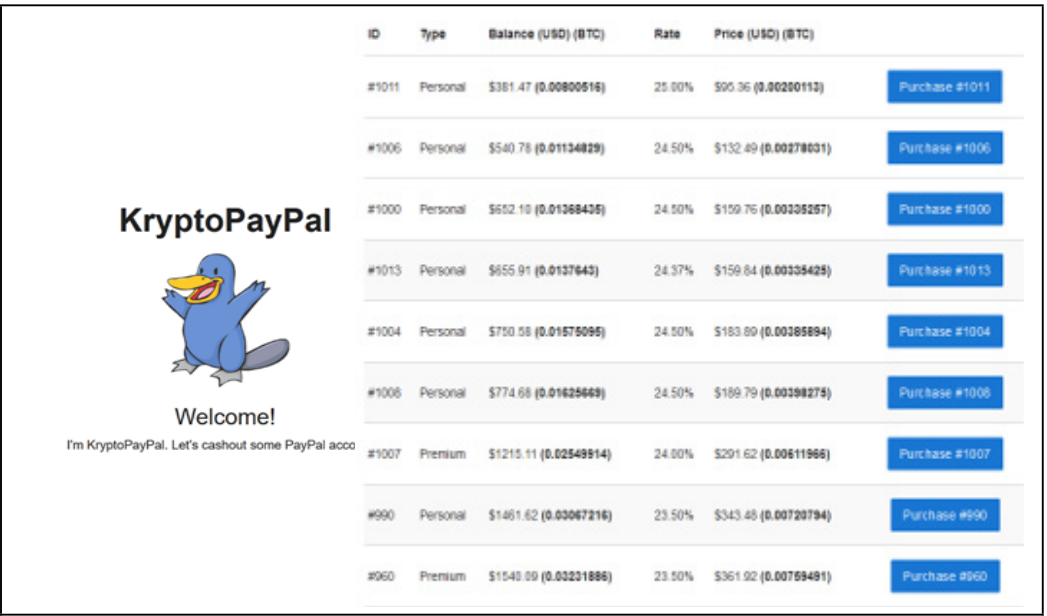
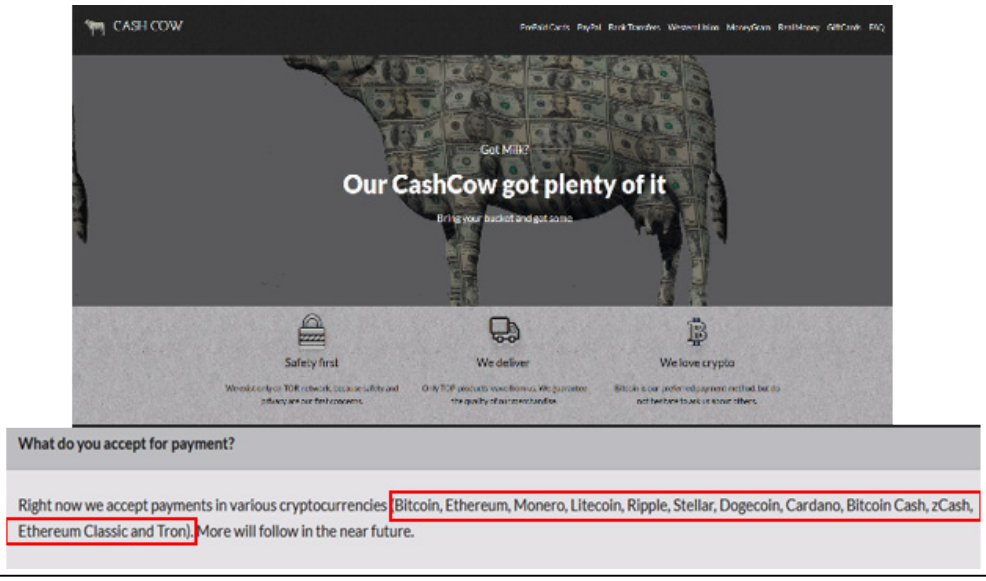
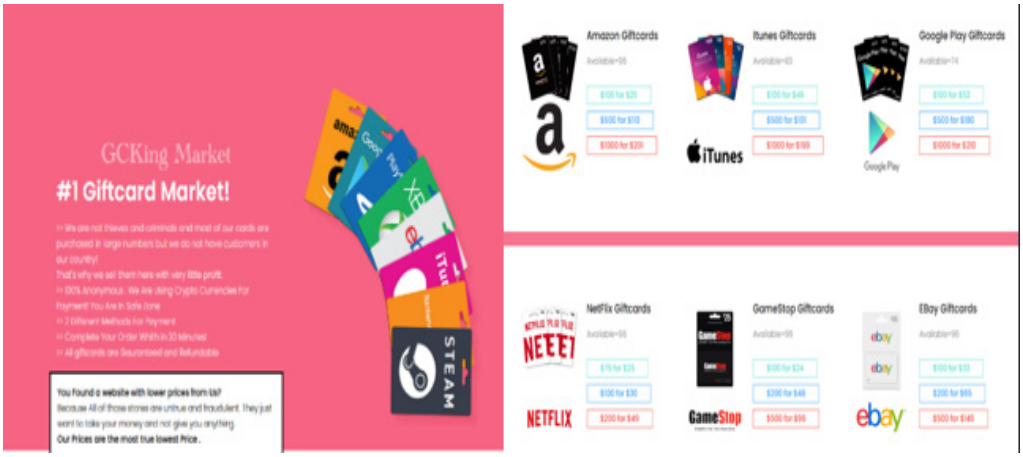
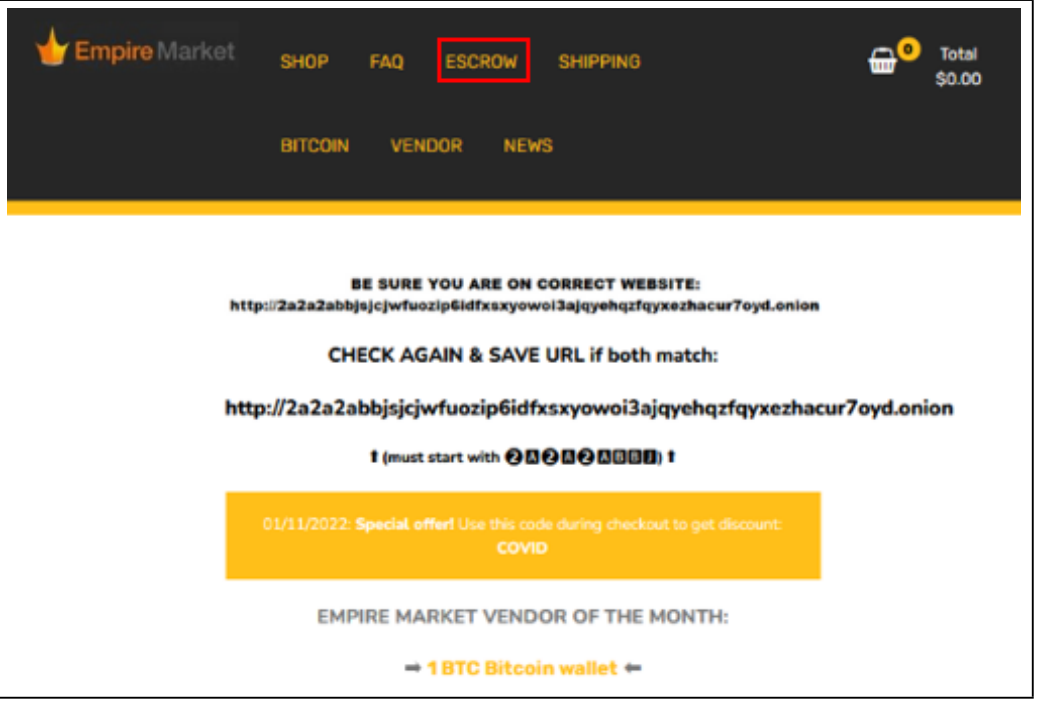
1. Krypto PayPal	
2. Cash Cow Payment	

Figure 1-4 Dark Web Financial Vendors

3. Gift Cards	
4. Escrow	

Pricing

Each vendor sets prices differently and has its pricing strategy, but there is a consensus on similar products/services' prices. This vendor (#3) advertises and sells credit cards. This vendor (#3) advertises and sells credit cards. The customer service includes chipped and magnetic credit cards (American Express, Visa, and Mastercard), card PINs, and conversion of the card to the purchaser's local currency. For example,

BITCARDS, started in 2021 and verified by Hidden Wiki, offers prepaid American Express and Visa cards. This vendor also offers discounts for the purchase of multiple cards. Purchasing three cards yields a 10% discount, purchasing five cards a 20% discount (one free card), and purchasing ten cards a 30% discount (three free cards).

Figure 5. Design of Cards (vendor #3)

The vendor (#3) uses a competitive pricing strategy to attract customers. Discounts increase as more cards are purchased. Different card types and currencies have different starting prices. For credit cards with USD, CAD, and AUD currencies, for example, card prices start from $130; for credit cards with EUR and GBP currencies, prices start from $150. However, the price of American Express cards starts from $250 and increases to $3,700 if the customer purchases 20 cards. The price ranges of these three different card schemes are presented in Figure 6.

This vendor (#3) offers a wide range of payment methods, including Bitcoin, Ethereum, Ripple, Western Union, Litecoin, Monero, Stellar Lumens, and Transferwise. Three shipping options are available: regular shipping (5-7 days in any country), express shipping (2–3 days to deliver, available in most countries), and overnight shipping (an additional $30 and available only in Mexico, the USA, and Canada). In addition, to ensure consumer trust, the vendor (#3) notes that the website, which has existed since 2012, is verified by Hidden Wiki.

Winning Customers' Trust

In Dark Web and illicit marketplaces, as in all marketplaces, building trust between vendors and buyers is essential (Laferrière & Décary-Hétu, 2022; Nijhuis, 2022; Norbutas, 2020; Paoli et al., 2017; Tzanetakis et al., 2016). Vendors only establish vendor shops to host sales (Paoli et al., 2017). Customers who wish to purchase cryptocurrency directly from these vendors do not rely on third-party services provided by crypto markets. Consequently, vendors can avoid commission charges on their sales and exposure to the financial risk of crypto market "exit scams" (Paoli et al., 2017).

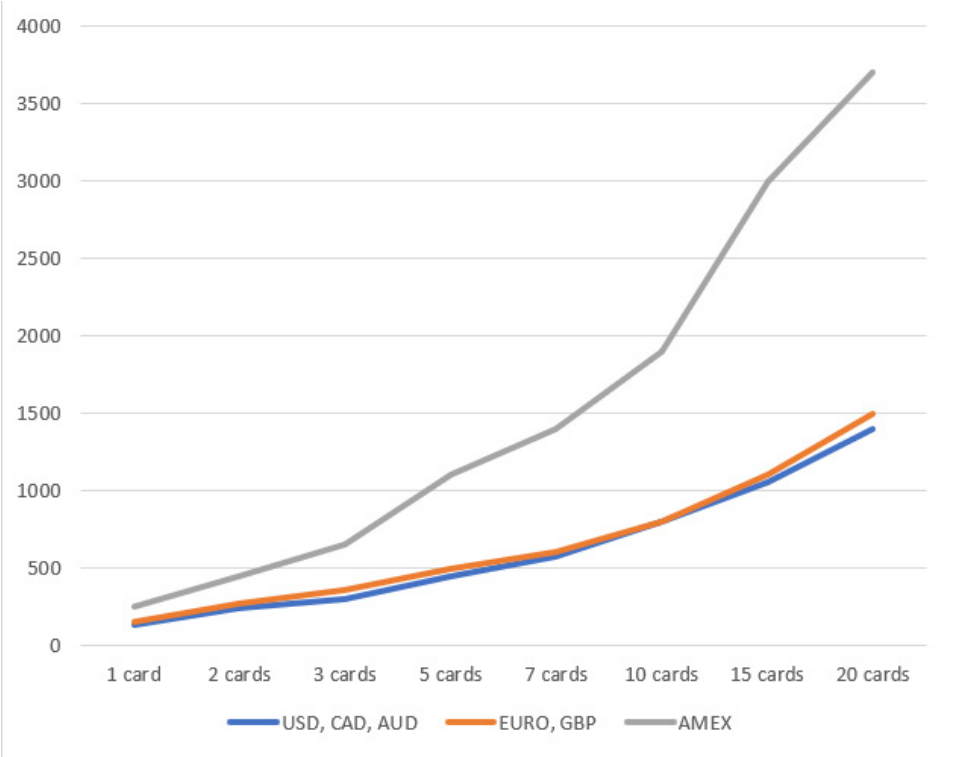


Figure 6. Pricing Schemes of the Vendor (#3)

Years of experience and Hidden Wiki verification are the primary means by which Dark Web sellers advertise themselves as "trusted vendors." Technically, these claims are effective ways of forging trust between vendors and sellers. However, in reality, at least based on the current data, they are also ways of disguising vendor fraud.

Bitcoin site No. 119 references "the countless transactions [it has] handled in the past 4 years" and states that it is "virtually impossible to pinpoint the source and endpoint of the coins." However, this website is a scam (Bitcoin sites: No. 119). Similarly, Bitcoin site No. 10 states that "[their] website [is] verified by Hidden Wiki/Tor Links/Reddit/ Deep Dot Web." However, it is also a fraudulent vendor (Bitcoin sites: No. 10). This website also advertises that it has existed since 2014.

As another example, BITCARDS posts a warning message to inform customers about scams run on other websites in Figure 3. At the same time, the vendor confidently states that customers must decide for themselves whom to transact with and that they are the sole persons responsible for their wealth.

Discussion

The study aims to examine target suitability components to uncover (1) what main products scammers

encourage customers to purchase, (2) how financial market vendors operate their business, and (3) which marketing strategies are used to scam potential buyers in the Dark Web financial market. The study identifies a few financial products that are most likely to be a scam in the Dark Web market. The main product that scammers encourage customers to purchase is PayPal Transfer, while Cloned Cards and Cryptocurrency Laundry are less likely to be scam products. However, Cryptocurrency Laundry was founded less than two years ago, which explains a relatively small amount of scam reports.

These findings indicate that most of the cryptocurrencies examined in the study are not strongly associated with scam activities except Monero, which is more likely to be a scam. After the FBI successfully seized the Colonial Pipeline hacker's Bitcoin transactions, Monero earned popularity, as an alternative to Bitcoin, with solid security. The anonymity of Monero provided a safe environment to the scam sellers with low risks of getting caught. Although the former underground marketplace Alpha Bay has argued that Monero is a more secure cryptocurrency than Bitcoin (Soska & Christin, 2015), the results indicate that purchasing financial goods using Monero is not secure for customers. This finding concludes that scam sellers are likely to accept Monero as cryptocurrency.

The customer service, the Hidden Wiki verification that proves financial markets as a trusted vendor of the Dark Web markets are positively correlated with being a scam. Therefore, the findings support the claim that consumers who find advertisements credible are susceptible to fraud (McAlvanah et al., 2015).

The findings reinforce the importance of capable guardianship to prevent scam behaviors in Dark Web market financial services. As digital frauds are prevalent, SEC announced that cryptocurrencies must register with the SEC to prevent fraudulent and manipulative trading practices. In addition, SEC doubled the size of the Crypto Assets and Cyber Unit for investigating cryptocurrency fraud (SEC, 2017; 2018). The study results can be beneficial for developing effective formal and informal social control that prevents scam behavior in the Dark Web financial market with target-hardening activities.

Conclusion

The operation of illegal businesses and fraudulent behaviors targeting customers are prevalent in the Dark Web marketplace. The anonymous nature of Dark Web technology and cryptocurrencies allows Dark Web financial services to evade the regulations imposed by the authorities and the investigation of law enforcement agencies. To further understand Dark Web financial services, this study examined the characteristics of Dark Web financial services, their products and services, and scams harboring strategies against the buyers.

Information was collected from 117 financial market sites and 31 Escrow sites. Vendor characteristics were compared, and statistical and thematic analyses were employed to identify the factors associated with vendors reported as scammers. The regression results suggest that more than half of the financial marketplaces had been reported as scam vendors. Most Escrow services, which are used to ensure the safety of transactions between buyer and seller, were also found to be fraudulent. . The thematic analysis results demonstrated that payment type, the vendor's pricing strategy, and vendor–consumer trust-building are important predictors of scam vendors and create a profile of a victim's susceptibility to being scammed.

Although this study provides insights into the Dark Web market financial services, it is not without limitations. Due to the Dark Web's anonymity and security and the ever-changing nature of Dark Web marketplaces, the sample may not represent the true extent of Dark Web financial services. The data included only 117 cases of financial services and 31 cases of Escrow services; Further research should include a greater sample size to explore the scam culture of the Dark Web marketplace and determine future directions for fraud detection.

The findings suggest that fraudulent behaviors targeting customers are prevalent in the Dark Web financial marketplace with various operations. Considering routine activity theory, policy implications related to the current study focus on capable guardianship (Cohen & Felson, 1979). In formal social control, while the structure of Dark Web financial marketplace fraud formed is highly complex (Ablon et al., 2014), various techniques have been introduced to combat Dark Web market frauds (Bradley & Stringhini, 2019; Fidalgo et al., 2019; Gelber, 2006; White et al., 2019). Since fraudulent sellers in the Dark Web financial marketplace formed highly structured and sophisticated techniques (Ablon et al., 2014) and are hidden under anonymized darknet security (Buxton & Bingham, 2015), advanced level of investigation techniques and toolkits should be implemented for Dark Web investigation. In addition, encrypted cryptocurrency transactions using Dark Web security supports the efforts of cybercriminal's conducting illegal activities and creates new types of crypto-related cybercrime (Dion, 2013). Advanced investigation skills are required to follow the trail of illicit transactions and funds. Law enforcement agencies should focus on technical training to develop skilled agents to enhance their ability in Dark Web investigations. In addition, there is a lack of government regulations or sanctions to respond to fraud crimes on the Dark Web, which dependable effects on potential Dark Web fraud sellers (Geers, 2010). There are various existing practical training programs based on Surface Web. investigation (Newman & Clarke, 2003; Siponen et al., 2008; Wall, 2007a, 2007b; Yar, 2005). However, few training opportunities are available due to the limited resources of local and state law enforcement agencies. Law enforcement agencies should create legislation and sanctions to convict cyber-criminals who committed fraud crimes in the Dark Web marketplace. As Dark Web vendors are often located outside the United States (White et al., 2019), it is important that investigators and law enforcement become familiar with both traditional and international elements of cyber investigation.

For informal social control, opportunity-reducing techniques such as target hardening of information systems should be maintained by online retailers and Internet service providers (Newman & Clarke, 2003) in the Dark Web financial marketplace. In addition, techniques to increase risks and reduce rewards for fraud sellers should be developed and implemented (Clarke &Weisburd, 1994; Hesseling, 1995; Weisburd et al., 2006) in the Dark Web marketplace. Due to the Dark Web's market's characteristic of avoidance of government regulations or sanctions due to atomicity (Beckert & Wehinger, 2013), sellers utilizing the Dark Web marketplace freely commit fraud against their consumers. Therefore, each marketplace should punish or ban fraudulent sellers from any future activities and publicize a seller's identification won their websites when they receive reports or complaints from victims. To prevent fraud in the Dark Web financial market, organizations of each marketplace should supervise their registered sellers. Furthermore, Dark Web financial services consumers should be aware that trusting sellers can sometimes result in buyers being harmed (Samonas & Angell, 2010), especially due to inadequate monitoring or supervision (Dhillon & Moores, 2001) such as occurs in the Dark Web financial marketplace.

Moreover, public awareness programs should inform consumers that fraud detection is difficult to apply in unregulated illegal marketplaces. The public should be aware that more than half of cybercriminals, many who are experts in illegal transactions, can be scammed by those who transact with them. Those with minimal familiarity with transacting on the Dark Web, and even more experienced individuals, remain increasingly vulnerable to potentially purchasing fraudulent financial products. Lacking any form of federal regulations governing the Dark Web, victims who have been scammed have no recourse for reporting such scams, nor are there any avenues for seeking compensation if defrauded.

Regarding the nature of the Dark Web marketplace, a public awareness program was suggested to prevent the public from entering the Dark Web marketplace and becoming victimized by criminal activities. Target-hardening activity, and awareness programs can be effective tools to minimize damages from Dark Web financial market fraud and can play a crucial role in minimizing cybercrime victimization (Choi, 2015).

References

2021 Internet crime report. (2022). *Federal Bureau of Investigation, Internet Crime Complaint Centre (IC3), USA*.

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

Ahmadi, R., & Yang, B. R. (2000). Parallel imports: Challenges from unauthorized distribution channels. *Marketing Science, 19*(3), 279-294.

Ahvanooey, M. T., Zhu, M. X., Mazurczyk, W., Kilger, M., & Choo, K.-K. R. (2021). Do Dark Web and Cryptocurrencies Empower Cybercriminals?

Akers, R. L. (2013). *Criminological theories: Introduction and evaluation*. Routledge.

Aldridge, J., & Decary-Hétu, D. (2015). Cryptomarkets and the future of illicit drug markets. In The *Internet and drug markets* (pp. 23-32). Publications Office of the European Union.

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

Anderson, R., Barton, C., Böhme, R., Clayton, R., Van Eeten, M. J., Levi, M., Moore, T., & Savage, S. (2013). Measuring the cost of cybercrime. In *The economics of information security and privacy* (pp. 265-300). Springer.

Assets. Retrieved from U.S. Securities and Exchange Commision. https://www.sec.gov/news/public-statement/enforcement-tm-statement-potentially-unlawful-online-platforms-trading

Bajari, P., & Hortaçsu, A. (2004). Economic insights from internet auctions. *Journal of Economic Literature, 42*(2), 457-486.

Banday, M. T., & Qadri, J. A. (2011). Phishing-A growing threat to e-commerce. *arXiv preprint arXiv:1112. 5732*.

Barratt, M. J. (2012). Silk Road: Ebay for drugs: The journal publishes both invited and unsolicited letters. *Addiction, 107*(3), 683-683.

Barratt, M. J., Allen, M., & Lenton, S. (2014). "PMA sounds fun": Negotiating drug discourses online. *Substance Use & Misuse, 49*(8), 987-998.

Beckert, J., & Wehinger, F. (2013). In the shadow: Illegal markets and economic sociology. Socio-Economic Review, 11(1), 5-30. Bradley, C., & Stringhini, G. (2019). A qualitative evaluation of two different law-enforcement approaches on dark net markets. 2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW) (pp. 453-463). IEEE.

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative research in psychology, 3*(2), 77-101.

Broadhurst, R., Grabosky, P., Alazab, M., Bouhours, B., Chon, S., & Da, C. (2013). Crime in cyberspace: offenders and the role of organized crime groups. *Available at SSRN 2211842*.

Brown, J., & Morgan, J. (2006). Reputation in online auctions: The market for trust. *California Management Review, 49*(1), 61-81.

Button, M., Nicholls, C. M., Kerr, J., & Owen, R. (2014). Online frauds: Learning from victims why they fall for these scams. *Australian & New Zealand journal of criminology, 47*(3), 391-408.

Buxton, J., & Bingham, T. (2015). The rise and challenge of dark net drug markets. *Policy brief, 7*(2), 1-24.

Byrne, D. (2021). A worked example of Braun and Clarke's approach to reflexive thematic analysis. *Quality & Quantity*, 1-22.

Castells, M. (2002). *The Internet galaxy: Reflections on the Internet, business, and society*. Oxford University Press on Demand.

Chikada, A., & Gupta, A. (2017). Online brand protection. *In Handbook of Research on Counterfeiting and Illicit Trade*. Edward Elgar Publishing.

Choi, K. S. (2008). Computer crime victimization and integrated theory: An empirical assessment. *International Journal of Cyber Criminology, 2*(1).

Choi, K. S. (2010). *Risk factors in computer-crime victimization*. LFB Scholarly Pub..

Choi, K. (2015). *Cybercriminology and digital investigation*. LFB Scholarly Publishing.

Choi, S. (2018). Illegal Gambling and Its Operation via the Darknet and Bitcoin: An Application of Routine Activity Theory. In *BSU Master's Theses and Projects*. Item 64.

Christin, N. (2013). Traveling the Silk Road: A measurement analysis of a large anonymous online marketplace. Proceedings of the 22nd international conference on World Wide Web (pp. 213-224).

Clarke, R. V., & Weisburd, D. (1994). Diffusion of crime control benefits: Observations on the reverse of displacement. *Crime Prevention Studies, 2*(1), 165-184.

Clarke, V., & Braun, V. (2013). Teaching thematic analysis: Overcoming challenges and developing strategies for effective learning. *The Psychologist, 26*(2).

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

DeLiema, M., & Witt, P. (2021). Mixed Methods Analysis of Consumer Fraud Reports of the Social Security Administration Impostor Scam.

DeLiema, M., Li, Y., & Mottola, G. R. (2021). Correlates of compliance: Examining consumer fraud risk factors by scam type. *Available at SSRN 3793757*.

Dhillon, G., & Moores, S. (2001). Computer crimes: theorizing about the enemy within. *Computers & Security, 20*(8), 715-723.

Dini, F., & Spagnolo, G. (2009). Buying reputation on eBay: Do recent changes help? *International Journal of Electronic Business, 7*(6), 581-598.

Dion, D. A. (2013). I'll gladly trade you two bits on Tuesday for a byte today: Bitcoin, regulating fraud in the e-conomy of Hacker-cash. *U. Ill. JL Tech. & Pol'y*, 165.

Drew, J., & Moore, T. (2014). Automatic identification of replicated criminal websites using combined clustering. 2014 IEEE Security and Privacy Workshops (pp. 116-123). IEEE.

Elbahrawy, A., Alessandretti, L., Rusnac, L., Goldsmith, D., Teytelboym, A., & Baronchelli, A. (2020). Collective dynamics of Dark Web marketplaces. *Scientific Reports, 10*(1), 1-8.

Fidalgo, E., Alegre, E., Fernández-Robles, L., & González-Castro, V. (2019). Classifying suspicious content in tor darknet through Semantic Attention Keypoint Filtering. *Digital Investigation, 30,* 12-22.

Geers, K. (2010). The challenge of cyber attack deterrence. *Computer Law & Security Review, 26*(3), 298-303.

Gelber, A. (2006). Federal jurisdiction in child pornography cases. *US Att'ys Bull., 54,* 3.

Georgoulias, D., Pedersen, J. M., Falch, M., & Vasilomanolakis, E. (2021). A qualitative mapping of Dark-web marketplaces. 2021 APWG Symposium on Electronic Crime Research (eCrime) (pp. 1-15). IEEE

Goldfeder, S., Bonneau, J., Gennaro, R., & Narayanan, A. (2017). Escrow protocols for cryptocurrencies: How to buy physical goods using bitcoin. International Conference on Financial Cryptography and Data Security (pp. 321-339). Springer, Cham.

Grabosky, P. (2000). Computer crime: A criminological overview. Workshop on Crimes Related to the Computer Network, 10th United Nations Congress on the Prevention of Crime and the Treatment of Offenders. Vienna. 2000.

Hesseling, R. (1995). Displacement: A review of the empirical literature, Crime Prevention Studies. In: Criminal Justice Press, New York.

Ilievski, A., & Bernik, I. (2016). Social-economic aspects of cybercrime. *Peer-reviewed academic journal Innovative Issues and Approaches in Social Sciences.*

Kadlecová, L. (2015). Russian-speaking cybercrime: reasons behind its success. *Eur Rev Organised Crime, 2*(2), 104-121.

Kaefer, F., Roper, J., & Sinha, P. N. (2015). A software-assisted qualitative content analysis of news articles: Examples and reflections.

Koch, R. (2019). Hidden in the Shadow: The Dark Web-A Growing Risk for Military Operations? 2019 11th International Conference on Cyber Conflict (CyCon) (Vol. 900, pp. 1-24). IEEE.

Laferrière, D., & Décary-Hétu, D. (2022). Examining the Uncharted Dark Web: Trust Signalling on Single Vendor Shops. Deviant Behavior, 1-20.

Lea, S. E., Fischer, P., & Evans, K. M. (2009). The psychology of scams: Provoking and committing errors of judgement.

Lee, C. S. (2022). Analyzing Zoombombing as a new communication tool of cyberhate in the COVID-19 era. *Online Information Review, 46*(1), 147-163.

Lee, S., Yoon, C., Kang, H., Kim, Y., Kim, Y., Han, D., Son, S., & Shin, S. (2019). Cybercriminal minds: an investigative study of cryptocurrency abuses in the Dark Web. 26TH ANNUAL NETWORK AND DISTRIBUTED SYSTEM SECURITY SYMPOSIUM (NDSS 2019) (pp. 1-15). Internet Society.

Leech, N. L., & Onwuegbuzie, A. J. (2011). Beyond constant comparison qualitative data analysis: Using NVivo. *School Psychology Quarterly, 26*(1), 70.

Leukfeldt, E. R., & Yar, M. (2016). Applying routine activity theory to cybercrime: A theoretical and empirical analysis. *Deviant Behavior, 37*(3), 263-280.

Lusthaus, J. (2020). Cybercrime in Southeast Asia.

Maguire, M., & Delahunt, B. (2017). Doing a thematic analysis: A practical, step-by-step guide for learning and teaching scholars. *All Ireland Journal of Higher Education, 9*(3).

Martin, J. (2014). Lost on the Silk Road: Online drug distribution and the 'cryptomarket'. *Criminology & Criminal Justice, 14*(3), 351-367.

McAlvanah, P., Anderson, K. B., Letzler, R., & Mountjoy, J. (2015). Fraudulent advertising susceptibility: an experimental approach. *Available at SSRN 2593898.*

Mirea, M., Wang, V., & Jung, J. (2019). The not so dark side of the darknet: A qualitative study. *Security Journal, 32*(2), 102-118.

Nardo, M. (2011). Economic crime and illegal markets integration: a platform for analysis. *Journal of Financial Crime*, Vol. 18 No. 1, pp. 47-62 .

Newman, G. R., & Clarke, R. V. (2003). *Superhighway robbery*. Willan.

Nicholls, J., Kuppa, A., & Le-Khac, N.-A. (2021). Financial Cybercrime: A Comprehensive Survey of Deep Learning Approaches to Tackle the Evolving Financial Crime Landscape. *IEEE Access.*

Nijhuis, S. (2022). *Dark Web markets: what can they teach us*? (Bachelor's thesis/University of Twente.

Norbutas, L. (2020). *Trust on the Dark Web: An analysis of illegal online drug markets* (Doctoral dissertation, Utrecht University).

Nunes, E., Diab, A., Gunn, A., Marin, E., Mishra, V., Paliath, V., ... & Shakarian, P. (2016, September). Darknet and deepnet mining for proactive cybersecurity threat intelligence. In 2016 IEEE Conference on Intelligence and Security Informatics (ISI) (pp. 7-12). IEEE.

Onkvisit, S., & Shaw, J. J. (1989). The international dimension of branding: strategic considerations and decisions. *International Marketing Review*.

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.

Piazza, F. (2016). Bitcoin in the Dark Web: a shadow over banking secrecy and a call for global response. *S. Cal. Interdisc. LJ, 26*, 521.

Pieters, G., & Vivanco, S. (2017). Financial regulations and price inconsistencies across Bitcoin markets. Information Economics and Policy, 39, 1-14.

Rudesill, D. S., Caverlee, J., & Sui, D. (2015). The deep web and the darknet: A look inside the internet's massive black box. *Woodrow Wilson International Center for Scholars, STIP, 3.*

Samonas, S., & Angell, I. O. (2010). The power of discretion in IS security. *Journal of Information System Security, 6*(2), 3-29.

Schafer, J. L., & Graham, J. W. (2002). Missing data: our view of the state of the art. *Psychological Methods, 7*(2), 147.

SEC. (2017). *SEC Nearly Doubles Size of Enforcement's Crypto Assets and Cyber Unit* https://www.sec.gov/news/press-release/2022-78

SEC. (2018). Statement on Potentially Unlawful Online Platforms for Trading Digital

Siponen, M., Willison, R., & Baskerville, R. (2008). Power and practice in information systems security research. *ICIS 2008 Proceedings,* 26.

Snyder, J. M. (1999). Online auction fraud: are the auction houses doing all they should or could stop online fraud. *Fed. Comm. LJ, 52*, 453.

Soska, K., & Christin, N. (2015). Measuring the longitudinal evolution of the online anonymous market place ecosystem. 24th USENIX Security Symposium (USENIX Security 15) (pp. 33-48).

Szakonyi, A., Leonard, B., & Dawson, M. (2021). Dark Web: A Breeding Ground for ID Theft and Financial Crimes. In *Handbook of Research on Theory and Practice of Financial Crimes* (pp. 506-524). IGI Global.

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.

Verizon. (2016). *2021 Data Breach Investigations Report.* https://conferences.law.stanford.edu/cyberday/wp-content/uploads/sites/10/2016/10/2b_Verizon_Data-Breach-Investigations-Report_2016_Report_en_xg.pdf.

Wall, D. (2007a). *Cybercrime: The transformation of crime in the information age* (Vol. 4). Polity.

Wall, D. (2007b). Policing Cybercrimes: Situating the Public Police in Networks of Security within the Cyberspace'Police Practice and Research. An International Journal.

Waters, R. (2003). How fraudsters set traps and take the credit. *Financial Times*, 1.
Wątorek, M., Drożdż, S., Kwapień, J., Minati, L., Oświęcimka, P., & Stanuszek, M. (2021). Multiscale characteristics of the emerging global cryptocurrency market. *Physics Reports, 901*, 1-82.
Weber, J., & Kruisbergen, E. W. (2019). Criminal markets: the Dark Web, money laundering and counter-strategies-An overview of the 10th Research Conference on Organized Crime. *Trends in Organized Crime, 22*(3), 346-356.
Weisburd, D., Wyckoff, L. A., Ready, J., Eck, J. E., Hinkle, J. C., & Gajewski, F. (2006). Does crime just move around the corner? A controlled study of spatial displacement and diffusion of crime control benefits. *Criminology, 44*(3), 549-592.
White, R., Kakkar, P. V., & Chou, V. (2019). Prosecuting darknet marketplaces: Challenges and approaches. *Dep't of Just. J. Fed. L. & Prac., 67*, 65.
Whitty, M. T., & Buchanan, T. (2012). The online romance scam: A serious cybercrime. *CyberPsychology, Behavior, and Social Networking, 15*(3), 181-183.
Yar, M. (2005). The Novelty of 'Cybercrime' An Assessment in Light of Routine Activity Theory. *European Journal of Criminology, 2*(4), 407-427. Yetter, R. B. (2015). Darknets, cybercrime & the onion router: Anonymity & security in cyberspace (Doctoral dissertation, Utica College).
Yu, B., & Singh, M. P. (2000). A social mechanism of reputation management in electronic communities. International Workshop on Cooperative Information Agents (pp. 154-165). Springer, Berlin, Heidelberg.
Yu, B., & Singh, M. P. (2002). An evidential model of distributed reputation management. In Proceedings of the first international joint conference on Autonomous Agents and Multiagent Systems: Part 1 (pp. 294-301).
Zhang, G., Li, Z., Huang, J., Wu, J., Zhou, C., Yang, J., & Gao, J. (2022). efraudcom: An e-commerce fraud detection system via competitive graph neural networks. *ACM Transactions on Information Systems (TOIS), 40*(3), 1-29.
Zhang, Y., Bian, J., & Zhu, W. (2013). Trust fraud: A crucial challenge for China's e-commerce market. *Electronic Commerce Research and Applications, 12*(5), 299-308.