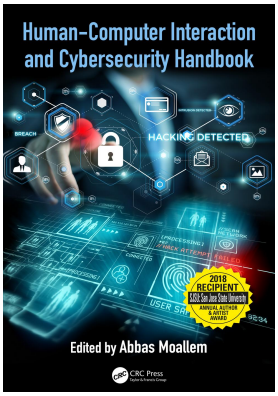

Human-Computer Interaction and Cybersecurity Handbook

Abbas Moallem

Money laundering and black markets

Publication details
https://test.routledgehandbooks.com/doi/10.1201/b22142-8
Brita Sands Bayatmakou
Published online on: 24 Oct 2018

chapter eight

Money laundering and black markets

Brita Sands Bayatmakou

Contents

8.1 Introduction

This chapter will provide an overview of money laundering and the interplay with cyber-criminal activity. The subject of today's black markets that increasingly facilitate and enable these crimes will be covered in the second half of the chapter.

As described in previous chapters, cyber-related crimes have increased exponentially in recent years. After gaining an understanding of who and what is behind the data breaches and cyberattacks as well as the tactics used to commit cyber-related crime, it is important to understand how the stolen information, assets, or even identities are bought and sold and how the proceeds are laundered. Choking off a criminal organization's

ability turn a profit through underground markets is arguably one of the most important deterrents. If the venue and methods to obscure and move illegally obtained funds are removed, the benefit to pursue such criminal activity no longer outweighs the cost. Case examples will be provided in the second half of this chapter.

Almost all profit-generating crimes involve money laundering as a means to disguise illicit proceeds and integrate them into the legitimate economy. Organized criminal networks that engage in a range of activities including, but not limited to, drug trafficking, human smuggling, embezzlement, insider trading, bribery, terrorism, illegal gambling, and cybercrime employ money laundering techniques to maintain their highly lucrative operations. The laundering of proceeds is arguably the most important aspect of any criminal enterprise as it ensures that profits make their way back to the criminal's pocket without being identified, reported, or ultimately seized by law enforcement. Criminals do this by disguising the sources, changing the form, or transferring the funds where it is unlikely to attract attention. According to the United Nations Office on Drugs and Crime (UNODC), criminals launder an estimated $1.6 trillion, or 2.7% of the global gross domestic product in 1 year. Less than 1% of global illicit financial flows are currently seized by authorities (UNODC 2011). The magnitude of illicit funds generated and the extent to which they are laundered through today's globalized systems has certainly risen with the increasing technological advancements, connectivity, and integration of the financial services industry. Thus, the statistics quoted earlier should be considered conservative figures.

8.1.1 *Money laundering defined*

Money laundering is the act of concealing the illegal origins of money derived from criminal activities and making those illegally gained profits appear legal or "clean." Criminals attempt to make the proceeds appear legal by misusing financial institutions and by employing complex methods to mask the origin, movement, and destination of such ill-gotten gains (Sharman 2011). Money is introduced or "placed" into the legitimate financial system, often transferred from any institution that facilitates financial transactions to another to obscure the source of funds, and is ultimately integrated into the formal economy to appear clean or legitimate.

In addition to undermining the legitimacy of financial systems and governments, money laundering imposes adverse macroeconomic impacts on society, threatening the safety and soundness of the global financial system. These significant impacts include distorting markets, imposing odious debt, contaminating the financial sector, destabilizing and creating counterintuitive capital flows, asset price bubbles, undermining the reputation of local institutions, and unfair competition. Much of this has a corrosive effect on the economy, government, and social well-being of a country and can impede investment and economic growth. The adverse socioeconomic impacts of money laundering include the perpetuation and promotion of criminal activities; corruption; drug abuse (in the case of laundering drug proceeds); and transfer of power from citizens, the market, and government to criminals.

8.1.2 *Money laundering in the twenty-first century*

It is important to distinguish today's money laundering methods and popular crimes from those of the past. Today, an increasing portion of illicit funds are generated through cyber-enabled crimes, defined as an illegal activity that is carried out or facilitated through electronic systems and devices, such as networks and computers. Thus, professional money

laundering services are in high demand. Perhaps the most disturbing trend is that cyberattackers are innovating much faster than those who defend against such attacks. Criminals today are reusing malware and adapting their products to stay ahead of the antimalware, antifraud, and anti-money laundering (AML) industries. This means that the role that governments and the private sector play in enhancing both AML and cybersecurity risk management policies will be critical to combating today's new and evolving threat landscape.

In many ways, however, cybercriminals are no different from other criminals involved in more "traditional" illegal activities such as drug or weapons trafficking. Like other organized crime groups, cybercrime enterprises function as well-funded businesses with an ultimate goal of making as large a profit as possible. Like a drug trafficker who must conceal the source and destination of drug sales, a cybercriminal must maintain strong partnerships and well-run supply chains. Unlike their legitimate counterparts, illegitimate enterprises must hire specialized employees to assist in laundering the business proceeds. Whether launching malicious software, harvesting an individual's credentials through a phishing e-mail, or demanding a ransom in Bitcoin in return for restored access to one's computer, these operations are only profitable if they are able to collect, obscure, and move the earnings. Also, like other traditional criminals, cybercriminals will always pursue the path of least resistance, migrating toward those activities that yield high rewards for relatively low risk and low cost. The lower risk offered in the cybercrime space has yielded a high demand for goods and services such as user credentials (usernames and passwords), personally identifiable information (PII), nonpublic information (NPI), exploit kits, and malicious software (malware), among many others.

The scale and size of cyber-related crime have grown dramatically and, according to a global economic crime survey, have become the second most reported crime (PwC 2018). Cyberattacks take a heavy toll on the economy, with corporate data breaches costing companies millions of dollars. The revenue from cyberrelated crime dwarfs that of the illegal drug trade, which clearly demonstrates how attractive this field is for criminals operating in the twenty-first century.

Without the dangers that accompany street-level criminal enterprises and a low likelihood that illicit profit will be seized, crimes perpetrated over electronic channels present a new frontier for professional money launderers. The reliance on electronic channels to move money and information has created opportunities for criminals. Indeed, many have pivoted their enterprises to leverage this shift by incorporating cyber tactics, techniques, and procedures (TTPs) into their illicit activities and by either committing cyber-enabled crimes themselves or using cybertools to facilitate unlawful acts such as money laundering. Technological advancements provide a greater reach for criminals to use the Internet and offshore servers to perpetrate crimes such as phishing, Internet auction fraud, romance scams, advanced fee fraud schemes, and fraudulent access to electronic digital media [computers, mobile devices, or Internet protocol (IP)-based phone systems] with a much broader impact. Thus, it should come as no surprise that business is good for cyberhackers and their support networks today. As society becomes more dependent on technology and innovation and as electronic channels are the primary medium through which crimes are committed, the scope for professional money laundering services will expand.

The most common methods to execute illicit transfers and attempt to launder proceeds today through financial institutions include the following (Figure 8.1):

- Wire and automated clearing house (ACH) fraud
- Credit card fraud
- Paper instrument fraud

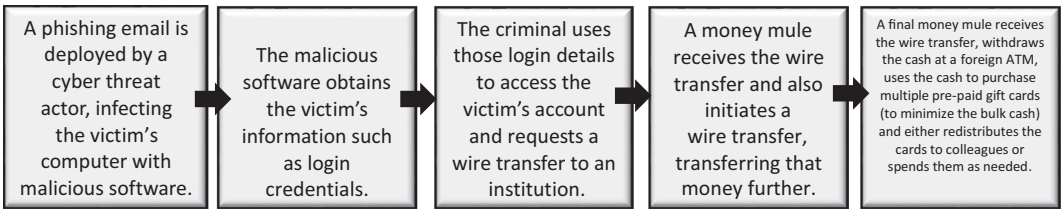

Figure 8.1 The scenario demonstrates how the financial proceeds of cybercrimes and fraud crimes may be laundered.

- Securities transactions
- Emerging payment networks such as prepaid access cards, peer-to-peer payments, crowdfunding, and microlending
- Cryptocurrencies and anonymous or encrypted transactions

One very popular way that cybercriminals can move their money is through micro-laundering, which makes it possible to launder a large amount of money in small amounts through thousands of electronic transactions. Financial institutions have systems that detect anomalous activity but may choose to focus on the relatively larger money movements. Emerging payment technology, such as PayPal and Venmo, or job advertising sites are popular for transferring small sums that may evade detective thresholds. Moreover, since online and mobile micropayments are interconnected with traditional payment services, funds can be moved through a variety of payment channels, increasing the difficulty to apprehend money launderers. One scenario might include the use of virtual credit cards as an alternative to prepaid mobile cards. The "card" is loaded using funds from a stolen bank account and an instant transfer can be sent using PayPal's network (Richet 2015).

8.2 *Anti-money laundering policy responses*

Given the devastating consequences of money laundering on society as a whole, it is increasingly important that organizations and governments work together to develop a response. The policies that have been developed to combat money laundering include legislative, regulatory, and investigative ones, which entail the collaboration of both the public and private sectors.

Many such policies have been similarly undertaken worldwide, and there are several bodies worth noting that are involved in anti-money laundering compliance and enforcement (Sharman 2011, p. 15). The Wolfsberg Group, an association of global banking institutions, aims to develop financial services industry standards relating to "know your customer (KYC)" anti-money laundering and counterterrorist financing policies. The Financial Action Task Force (FATF) is a policy-making body that promotes policies and measures to combat money laundering, the financing of terrorism, and proliferation of weapons of mass destruction. The FATF frequently publishes recommendations and papers on the topic. The Egmont Group is an international association of financial intelligence units that work to combat money laundering and terrorist financing through the exchange of expertise and information (Egmont Group 2018). The US Department of Treasury's Office of Foreign Asset Control administers laws that impose economic sanctions against entities that threaten US security. The UNODC, Basel Committee on Banking

Supervision, International Monetary Fund, and World Bank are other major institutions working to fight money laundering-related crimes.

Not surprisingly, financial institutions play an important role in helping investigative and regulatory agencies identify money laundering entities and take appropriate action. Because financial institutions are top targets, they are on the "front line" of defending the security and soundness of the economy and financial system by identifying and fighting fraud, money laundering, and the finance of terrorism. Compliance with US anti-money laundering legislation, particularly the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT Act), is a foundational component of risk management programs of banks, law firms, broker-dealers, asset management firms, auditors, money service businesses (MSBs), and other nonbank financial institutions. The USA PATRIOT Act has required banks and MSBs to comply with specific legislation. It has enabled the government to monitor information that helps counter criminal activity, thereby minimizing destabilizing impacts on the economy and security. While it provides a new layer of security, it also demands that banks implement strong internal compliance programs. Money laundering violations can bring serious penalties, may result in reputational damage, and, at worse, put a bank out of business.

The prevalence of cyber-related crimes in recent years has driven an industry-wide response with cybersecurity governance rising to the top of regulatory priorities alongside anti-money laundering compliance. Strengthening cybersecurity and anti-money laundering programs are key areas of focus for the Treasury Department (namely, the Office of the Comptroller of the Currency), the Financial Industry Regulatory Authority, the Securities and Exchange Commission, the Federal Reserve System, and the Federal Deposit Insurance Corporation (FDIC). The regulatory framework has shifted and expanded in the past 15 years to accommodate this ever-changing threat. To understand today's environment, it is worth outlining where the anti-money laundering regime started.

8.2.1 Money laundering regulation

The first legislation targeting money laundering crimes was the Bank Records and Foreign Transaction Reporting Act, also known as the Bank Secrecy Act (BSA). It was passed by the US Congress in 1970, requiring US financial institutions to collaborate with the US government in cases of suspected money laundering and fraud. According to the Treasury Department, the BSA established requirements for recordkeeping and reporting by private individuals, banks, and other financial institutions. It was designed to help identify the source, volume, and movement of currency and other monetary instruments transported or transmitted into or out of the United States or deposited in financial institutions. It imposed requirements for banks to report cash transactions over $10,000 using the currency transaction report, properly identify persons conducting transactions, and maintain a paper trail by keeping appropriate records of financial transactions. Under the BSA, financial institutions are obligated to assist the US government in the detection and prevention of money laundering, including by submitting suspicious activity reports (SARs) to report suspicious transactions or any series of transactions conducted or attempted that involve $5,000 or more in funds or other assets (Gup 2007). The BSA was implemented partly in response to income tax evasion and the concealment of assets that became commonplace through the use of bank accounts maintained in foreign jurisdictions. This was the first law of its kind and has served as one of the most important tools in combating money laundering by providing the Internal Revenue Service access to bank records, which has helped facilitate criminal and tax investigations that involve money laundering.

BSA data have also been used by a variety of US agencies such as the Federal Bureau of Investigation (FBI), the Department of Homeland Security, and the Drug Enforcement Administration. The Financial Crimes Enforcement Network (FinCEN), a bureau of the Treasury Department, acts as the designated administrator of the BSA and has contributed to its expanded use for investigations.

Many subsequent laws have enhanced and amended the BSA to provide law enforcement and regulatory agencies with the most effective tools to combat money laundering, and it remains the foundational framework with which institutions must comply. The following list of anti-money laundering laws have been implemented since 1970:

- BSA (1970)
- Money Laundering Control Act (1986)
- Anti-Drug Abuse Act of 1988
- Annunzio–Wylie Anti-Money Laundering Act (1992)
- Money Laundering Suppression Act (1994)
- Money Laundering and Financial Crimes Strategy Act (1998)
- USA PATRIOT Act
- Intelligence Reform and Terrorism Prevention Act of 2004

8.2.2 USA PATRIOT Act

The legislation introduced after the 9/11 terrorist attacks strives to further prevent pervasive financial criminal activity associated with terrorism. The USA PATRIOT Act was enacted to prevent and deter terrorist acts and to enhance law enforcement investigatory tools. The act strengthened special measures for certain jurisdictions, financial institutions, or international transactions of "primary money laundering concern" to detect and prosecute international money laundering and the financing of terrorism.

As noted, the BSA requires financial institutions to establish effective ways to detect, monitor, and report suspicious activity and to keep records and file reports that are determined to have a high degree of usefulness in preventing money laundering that may be a part of a criminal enterprise, terrorism, tax evasion, or other unlawful activity. Domestic and international law enforcement agencies leverage the documents filed under the BSA requirements to identify, detect, and deter money laundering (IRS 2017). Originally, this helped establish the "paper trail" that would build upon and enhance an investigation. With the advent of the Internet and the widespread use of technology to carry out electronic crimes, traditional reporting components have become less relevant. The paper trail has given way to the "digital footprint," a more useful forensic tool in today's environment.

8.2.3 Recent public policy developments: Cybersecurity and the financial services industry

Today's reliance on electronic channels to move money, communicate, and engage in financial transactions has created opportunities for criminals that are exacerbated by nascent security and cyber risk management programs. While the successful fraud or money laundering scheme still often relies on human error or the exploitation of a human component, the number of all financial crimes committed through electronic channels has outpaced any other method. The use of technology in financial services has expanded well beyond online banking and back-end computer systems. It now encompasses innovations

in financial services such as mobile payment applications, roboadvisers, peer-to-peer lending, and distributed ledger technology. The good news is that today's illicit financial activity is accompanied by data associated with a computer user's digital footprint, which may help investigators build networks of illicit actors and their associates, their activity, and related suspicious transactions. Examples of such data include device identification, IP addresses, time stamps, and indicators of compromise (IOCs).

Cybercrime is considered as one of the most significant threats targeting the financial services industry, and as cyberattacks become progressively more sophisticated and frequent, there is increasing pressure from financial services regulators to tighten cybersecurity governance and risk management. Recent high-profile cyberattacks on financial institutions have caused significant damage and highlight the concerns and challenges around the management of external threats and vulnerabilities. In response to the changing criminal landscape, several regulatory authorities issued guidance and regulations relating to cyber-related crime and attacks and took action, reflecting a focus on improving cybersecurity in the financial services industry.

8.2.4 Federal Financial Institutions Examination Council cybersecurity assessment tool

The Federal Financial Institutions Examination Council (FFIEC), an interagency group that coordinates the federal supervision of depository institutions, released a cybersecurity assessment tool in June 2015. In 2014 and 2015, the FFIEC also issued several joint statements on various types of cyberattacks, citing the increased risks around distributed denial-of-service (DDoS) attacks, malware, cyberextortion, automated teller machine (ATM), and card authorization systems. According to the FFIEC (2017), the aim of the tool is to "help institutions identify their risks and determine their cybersecurity preparedness. The Assessment provides a repeatable and measurable process for financial institutions to measure their cybersecurity preparedness over time."

8.2.5 FRB, OCC, FDIC Advanced notice of proposed rulemaking

On October 26, 2016, the board of governors of the Federal Reserve Bank (FRB), the Office of the Comptroller of the Currency, and the FDIC jointly published an advance notice of proposed rulemaking of the Enhanced Cyber Risk Management Standards (FRB 2016a). The stated goal of the three federal banking regulatory agencies in considering these enhanced standards is to strengthen the operational resilience of large and interconnected financial entities and, by doing so, reduce the likely impact of a cyberevent on the financial system as a whole. Under consideration by the agencies are five categories of cyber standards: cyber risk governance, cyber risk management, internal dependency management, external dependency management; and incident response, cyber resilience, and situational awareness. At the time of writing, the rule had not yet been published or finalized.

8.2.6 New York Department of Financial Services

At the state level, on September 28, 2016, the New York Department of Financial Services (NYDFS) published its proposed cybersecurity regulations as "first-in-the-nation" rules that would require all supervised entities including banks, insurers, and other financial services institutions to establish and maintain cybersecurity programs to protect consumers from cyberattacks "to the fullest extent possible" (NYDFS 2017). A year prior, the

NYDFS also issued regulations with specific standards for suspicious activity monitoring and watchlist screening by certain entities under its jurisdiction.

8.2.7 FinCEN guidances

Recent high-profile cyberattacks on financial institutions caused significant damage and highlighted the concerns and challenges around the management of external threats and vulnerabilities. FinCEN issued a targeted advisory notice on e-mail compromise fraud schemes in September 2016. Focusing on the impact to financial institutions, this advisory discussed schemes commonly referred to as business e-mail compromise (BEC), which target commercial customers and individuals' e-mail accounts (referred to as EACs). FinCEN cited FBI statistics that 22,000 cases were reported of BEC and EAC since 2013 involving $3.1 billion. These schemes focus on impersonating victims in order to submit seemingly legitimate transaction instructions for a financial institution to execute, rather than taking over the victim's actual account. FinCEN provided 11 examples of suspicious activity red flags that could help employees of institutions monitor for suspicious activity involving e-mail correspondence and fraudulent transaction instructions (FinCEN 2016a).

In October 2016, FinCEN released a more far-reaching advisory regarding cyberevents, cyber-enabled crime, and obligations of financial institutions for reporting under the BSA (FinCEN 2016b). The advisory provides interpretive guidance to financial institutions on the expectations of FinCEN with regard to the reporting of cyber-enabled crime and cyberevents and how to properly do so through SARs. Cyber-enabled crime encompasses illegal activities such as fraud, money laundering, or identity theft carried out or facilitated by electronic systems and devices, such as networks and computers. Cyberevents are defined as an attempt to compromise or gain unauthorized electronic access to electronic systems, services, resources, or information. Financial institutions targeted by the advisory include banks, casinos, money services businesses, broker-dealers, mutual funds, insurance companies offering particular types of insurance, futures commission merchants, introducing brokers in commodities, nonbank residential mortgage lenders or originators, and housing-related government-sponsored enterprises. Expanding the reporting requirement to include cyberevents and cyber-related information now provides critical pieces of information to form a "digital trail" that serves as a valuable source of leads to initiate investigations, identify criminals, and disrupt and dismantle criminal networks. The advisory indicates that relevant and available cyber-related information should be included in SARs. This includes technical details of electronic activity and behavior such as IP addresses with timestamps, IOCs, device identifiers, virtual wallet information, and methodologies used.

The advisory also requests that SARs relating to cyberevents should include a description of the magnitude of the event and the following information:

- Source and destination information, including the following:
  - IP address and port information with respective date time stamps in coordinated universal time
  - Attack vectors
  - Command-and-control nodes
- File information, including the following:
  - Suspected malware filenames
  - MD5, SHA-1, or SHA-256 hash
  - E-mail content

- Subject usernames, including the following:
  - E-mail addresses
  - Social media account/screen names
- System modifications, including the following:
  - Registry modifications
  - IOCs
  - Common vulnerabilities and exposures
- Involved account information, including the following:
  - Affected account information
  - Involved virtual currency accounts
- Known or suspected time, location, and characteristics or signatures of the event
- Other relevant IP addresses and their time stamps
- Device identifiers
- Methodologies used
- Other information the institution believes is relevant

It also encourages the collaboration within regulated institutions between BSA/AML, in-house cybersecurity departments, and fraud prevention teams to identify suspicious activity (Greene et al. 2016). Likewise, financial institutions should work with their peers, as outlined in Section 314(b), to identify threats, vulnerabilities, and criminals.

The following are examples of situations that would require the suspicious activity reporting to the Treasury Department:

- Malware intrusion that would put customer funds at risk
- Cyberevent that exposes sensitive customer information such as passwords, credit card numbers, or account numbers
- DDoS attack

Note that the standard may require the filing of SARs even in circumstances where no actual financial transactions ultimately occur or are attempted in connection with the cyberevent, indicating how crucial the government considers this information.

8.2.8 FRB, FDIC, and National Credit Union Administration guidances

Guidance was also issued by the board of governors of the FRB, the FDIC, and the National Credit Union Administration concerning the filing of SARs to report certain computer-related crimes (FRB 2016b; FDIC 1997; NCUA 1997).

The expanding requirements to enhance cybersecurity risk management efforts and leveraging of the anti-money laundering regulatory framework indicates an emphasis and priority by government institutions on these areas that is sure to remain for years to come.

8.3 Underground or black markets

A black market, underground economy, or shadow economy can be defined as an economic activity involving the buying and selling of merchandise or services illegally. The goods themselves may be illegal to sell, may be stolen, or may be otherwise legal goods sold illicitly to avoid taxes or licensing requirements (such as cigarettes or unregistered firearms). In this section, the terms *darknet markets*, *black markets*, and *underground markets*

refer to nonlegitimate marketplaces, and *dark web* refers to the location online where those underground markets exist.

Underground markets employ nearly half of the world's working population and have been a part of modern governance for centuries so it is important to take the past into account when describing today's environment. As has long been the case, black markets flourish, in part, by circumventing the rules and regulations put in place to create order. In early American history, much of the economy was based on smuggling and illicitly importing technological equipment and workers from England. Both legitimate businesses and criminal enterprises alike benefitted from the industrial revolution and later innovations, which brought conveniences such as steam power; machine tools; and eventually the railroad, the automobile, the telegraph, the radio, and cellular phone technology. The prohibition period in the early twentieth century in the United States serves as a great example of the creation of a black market and its return to legal trade. Many organized crime groups benefitted from banned alcohol production and sales, taking advantage of the fact that much of the populace did not view drinking alcohol as a particularly harmful activity. Illegal speakeasies prospered, and organizations such as the Mafia grew tremendously powerful through their black market alcohol distribution activities. Thus, when trying to picture a black market actor of the twentieth century, easily retrieved images include Italian mafiosos; Colombian drug lord and narco-terrorist Pablo Escobar; or a figure such as Viktor Bout, a Russian arms dealer known widely as the "merchant of death" for his delivery of weapons that aided and abetted many wars across the globe. Conversely, if asked to describe today's typical underground criminal, most would be hard pressed to provide a physical description of the "average hacker" or counterfeiting fraudster operating in the shadows of the dark web. Nevertheless, despite the technical, computerized, and digitized aspects of online black markets, the human factor remains the central component to business operations.

As described earlier in this chapter, globalization, technological advancements, and the Internet have created a more integrated global economic order, reducing barriers between financial networks and systems, facilitating growth, and increasing the speed at which transactions take place. As legitimate businesses benefit from the broadening opportunities resulting from such changes, so too are those who trade in illicit goods and services. Narcotics trafficking, sex tourism, computer hacking, money laundering, stolen artworks and antiquities, illegally harvested timber, oil, diamonds, counterfeit medicine, software, luxury brands (think very visible knock-off purse vendors on the streets of New York), and a globally networked market for human organs represent a multitrillion dollar global complex. These criminal activities still occur on the street but are increasingly moving online where the growing presence of underground markets in "cyberspace" facilitate the exchange of products between buyers and sellers who never have to interact. This has made it easier than ever for anyone to access illicit goods and services in the shadow markets that operate in anonymized and informal spaces.

This unregulated space presents a growing threat to businesses, governments, and consumers operating online because the activity has evolved from being a disparate and ad hoc group of networks to highly complex and well-organized operations with an increasingly sophisticated offering of products, tools, and services that help individuals carry out crimes, hide evidence of those crimes, and facilitate the laundering of the illicit proceeds. Where geography, physical presence, and face-to-face interactions built the trusted networks that defined black markets of the past, today's online underground economy is governed by anonymity and technology-based solutions. Although physical contact is largely absent, and despite the anonymization, secrecy, and the "dark" nature of today's online

black markets, as with traditional black market activity, the human component remains a pivotal component of the environment. Identity, alliances, and trust remain crucial to the markets' functioning.

Users establish relationships and gain comfort with a transaction through eBay-style or Yelp-style rating systems where an unreliable seller that delivers a "poor" product (or does not deliver at all) will be advertised as such. Market participants place orders and sell products, comfortably communicating thanks to the use of encryption, privacy, and cryptocurrencies (discussed more in the following sections). This allows users to build trust and feel more secure as they are protecting their communications and transactions. Web forums, e-mail, locked down social media, online stores, and instant messaging platforms exist as both private and open chat rooms. Transactions between suppliers, vendors, potential buyers, and intermediaries for goods or services are often fast and efficient with customer service that mirrors that of any legitimate business. In fact, buyers willingly pay a premium for good customer service and a guarantee that they are purchasing verified data such as credit card details or user logins. It is precisely these secure communications and the anonymization facilitating direct links between end users or customers all over the world that are attracting people to these markets and redefining the human dimension of today's "average" black market participant.

8.3.1 Anonymization, cryptography, and privacy

Defining the profile of today's underground economy actor presents a challenge for additional reasons. Given the rapid rise and fall of these markets in recent years allows little time for media, literature, or entertainment to study and document what the "typical" online criminal looks like. More importantly, the very feature making the business so attractive to a criminal also prevents the public from understanding his or her profile. The dark web keeps cybercriminals and money launderers afloat because it offers (often requires) anonymizing networks and untraceability. Such features impede the efforts of law enforcement, Internet service providers and financial intelligence units from detecting criminal activity, making this space a haven within which hackers and their criminal colleagues operate, almost with impunity. Obtaining a virtual private networks with strong encryption, using a proxy server, IP spoofing, and using the Onion Router (Tor) or the Invisible Internet Project (I2P) will hinder efforts to trace users' and administrators' online activity on unindexed sections of the web. TOR and I2P are free software and open networks that enable anonymous communication, file transfers, and Internet browsing that conceal a user's physical location preventing network surveillance or traffic analysis.

8.3.2 Crytpocurrencies

Digital cryptocurrencies and the use of distributed ledger technology (also known as the blockchain) are rapidly becoming the preferred method to value transfer for illicit goods and services, thus posing a number of money laundering risks. Developed in 2008, Bitcoin has become the most famous decentralized payment network. This cryptocurrency enables real-time, peer-to-peer payments to anyone in the world without the intermediation of a central authority or regulating country. This also means that individuals who hold cryptocurrencies have little to no recourse if fraud or theft occurs. Although Bitcoin is the most recognized cryptocurrency, there are hundreds of others, the most popular of which include Ethereum, Ripple, Litecoin, and Monero. Coinmarketcap.com (2017) provides the market capitalization and current price of the top cryptocurrencies

in circulation today. Cryptocurrencies are held and encrypted in various types of "wallets," both online and offline. Although not completely anonymous (all transactions are permanently stored on a traceable, public ledger), there is no requirement to store PII or for administrators to perform customer identification on these transactions unless formally registered with the US Treasury Department. Likewise, the pseudonymous nature of the "currency" makes it difficult for financial intelligence units or US-based virtual currency exchangers that are obligated under the BSA to identify and verify clients, to determine the counterparties involved in such transactions. Like other anonymizing elements of the dark web, cryptocurrencies make it difficult for law enforcement to trace, seize, and freeze illicit profits. This makes it attractive for actors operating on the black market.

There are many measures to further obscure funds transfers. Tumbling or mixing services offer a way to comingle a cryptocurrency transaction with many other transactions with the intention of confusing the source or origin of the funds. Another convenient tool for money launderers that emerged a few years after Bitcoin gained an increasing user base was a Bitcoin application to protect users' identities launched by a company called Dark Wallet. The application was described by its founder as "money-laundering software" (Greenberg 2014).

8.3.3 What is for sale?

The market forces that prevail on the dark or deep web also do so based on the same microeconomic concepts that have always driven legitimate markets. Prices go up with rising demands for products and services or when there is scarcity and go down when demand is low or supply is high. There is a healthy appetite today on underground markets for both stolen data and tools used to carry out malicious attacks, steal private data, or launder money. There is a range of products, information, and services available on the black market that enable cybercrimes and money laundering and that can be customized based on a buyer's needs. There is a substantial interest in goods such as hacking tools, digital assets, or "as-a-service" products such as money handling, obfuscation, and evading detection (Ablon et al. 2014).

The following are examples of products available on the black market. This nonexhaustive list is limited to cyber-related products and services. It does not include the sale of illegal substances, for example.

Stolen data

- Credit card information and personal identification numbers
- NPI
- TTPs
- E-mail logins and passwords
- Protected health information
- Personal information (social security number, date of birth, and identifying information used for authentication)
- Stolen identities

Services

It is important to keep in mind that criminals engaged on the dark web are well funded with professional business models that outsource a wide variety of services. In a noncentralized online system, characterized by greater flexibilities and agility, anyone can rent, lease, or purchase an as-a-service," which is a flourishing business

model run on black markets found on the darknet. Examples of an ever-expanding list are as follows:

- Data-as-a-service (data are stored in the cloud and is accessible by a range of systems and devices)
- Hacking-as-a-service
- DDoS-as-a-service
- Platform-as-a-services (to develop, run, and manage applications without the complexity of building and maintaining expensive infrastructure or launch applications)
- Ransomware-as-a-service
- Money laundering-as-a-service
- "Money handling services"
- Mule services (witting and unwitting money "mules")
- Fake website design (front companies)
- Shell company formation

Example products

- Malware
- Exploit kits
- Botnets for rent
- Hacking tools
- Tutorials on "how to blackmail for Bitcoin (ransomware)"

8.3.4 *Black market/dark web participants*

The ease with which market actors can get involved has increased over the years due to the array of available websites, forums, and chat channels that educate the average lay person on "how to hide your money trail," where to buy or sell credit card information, and other guides that lowers previous technical barriers to entry (Ablon et al. 2014, p. 4). Higher tiers of access to black markets require more vetting. Lower tiers might be publicly available open and require less vetting.

Indeed, hierarchies are established within these markets as well as specialized roles. Administrators occupy the most desirable position at the top and are followed by subject-matter experts who have sophisticated knowledge of particular areas (e.g., root kit creators, data traffickers, and cryptanalysts). Intermediaries, brokers, and vendors are next on the black market totem pole followed by the general membership. Each member may have a subsidiary cell of associated members (Ablon et al. 2014, p. 5). Other participants may include threat actors such as hacktivists or nonstate actors and freelancers.

As the incidence of data breaches and credit card theft online continues to rise, the general public has become virtually numb and apathetic to the high probability that their personal information such as that stored on a credit card has been stolen. When compromise occurs, a bank will promptly replace the card and reset the password, the consumer feeling little to no immediate impact, despite the fact that his or her credentials or personal information is now readily available for a relatively small price. To illustrate the demand, and thus the need, for awareness, Table 8.1 lists the estimated costs of credential and other data. Anyone who allows their data to be stored by a third party such as a healthcare provider or retailer (in other words, nearly the entire consumer population) should understand the high likelihood that their information could be compromised if a data breach occurs and will likely be sold on the black market. In 2016, one in three Americans had their healthcare data exposed. This is just one industry that happens to be more vulnerable

Table 8.1 Average underground prices for various hacker services

Hacker service	Average price
Visa or Mastercard credentials	$7.00
Credit card with magnetic stripe or chip data	$15.00
Premium American Express, Discover Card, Mastercard, or Visa with strip or chip data	$30.00
Bank account credentials (balance of $15,000)	$500
Bank account credentials (balance of $70,000–$150,000)	6% of account balance
Large US airline points accounts	1.5 million points cost $450
Large international hotel chain points account	1 million points cost $200[a]

Source: Cetera, M. *Prices Rise for Your Data on the Black Market*, http://www.bankrate.com/financing/credit-cards/prices-rise-for-your-data-on-the-black-market/, 2016.

than others, but the figure illustrates the scale and impact that these crimes can have on our society and the type of avenue for the compromise of highly personal information. Either an employee of the company will make a mistake resulting in data exposure or a determined cybercriminal will break through security defenses and steal sensitive information. The stolen information will likely be sold on a darknet market such as Alphabay, Silk Road 3, Dream Market, Crypto Market, or Ramp, among others.

8.3.5 Pursuing today's criminal

An advanced and evolving threat has also meant that law enforcement has had to shift its approach to combating these elements. Crime busting before the twenty-first century involved investigating individuals' patterns and associates as they moved through society. Today, an investigation is built around a digital footprint and the use of cyberforensics. Court-ordered search warrants to seize and attempt to search cellular phones, tablets, and other electronic devices, are helpful but often pose challenges for yet untrained investigators who may meet technical barriers. The following are a few examples for reference of how law enforcement has apprehended black market participants.

8.4 Silk Road and Operation Onymous: 2014

In 2014, an internationally coordinated law enforcement action, involving the Department of Justice, Department of Homeland Security, and law enforcement agencies of approximately 16 foreign nations working under the umbrella of Europol's European Cybercrime Centre and Eurojust, put an end to a half dozen top darknet sites, including Silk Road 2.0, targeting high-value actors of the dark web drug trade (FBI 2014). The bust occurred just a year after the takedown of the original Silk Road online marketplace that similarly offered a range of illegal goods and services including drugs, firearms trafficking, counterfeit goods, and fake passports. The website addresses, known as ".onion addresses," and computer servers hosting these websites, were seized as part of takedown, and 17 people were arrested. Although seen as a major success, other darknet sites, such as Agora, Evolution, and Andromeda remained online and intact, and warmly welcomed the new business that resulted from their competitor's demise. This "whack-a-mole" effect demonstrates the ongoing challenges faced by law enforcement in halting all underground market activity.

8.5 Bangladesh Bank: 2016

The largest bank robbery in history occurred in 2016 when $81 million was stolen from the Bangladesh central bank. Funds were sent from the account of the Bangladesh Bank at the Fed, then to several accounts that had been opened with false identification in May 2015 at Rizal Commercial Banking Corporation (RCBC) in the Philippines. Once received, RCBC wired them to a remittance company, Philrem Service Corporation, which then sent the money on to a number of Philippine casinos. From there, the authorities were unable to track the funds further. Experts believe the fraudsters installed malware at the Bangladesh Bank in January 2016. The company that investigated the attack discovered a malicious program in Bangladesh Bank's systems, which allowed the fraud actors to enter and systemically follow SWIFT transactions, disconnect a printer at the bank so that warnings regarding the transfers did not print, and hide or delete transactions in the system of the bank. The investigation linked the malicious code used in the heist to code used in both the Sony Pictures attack in 2014 and other bank attacks, including against several in South Korea (Fox-Brewster 2016). Many suspected that these attacks originated in North Korea.

Several other stories involving SWIFT-related wire frauds emerged in headlines shortly after the Bangladesh Bank events including an unsuccessful attempt through the Tien Phong Bank in Vietnam in December 2015 for $1.1 million and the theft of $9 million from a bank in Ecuador. Hackers also stole $10 million from an unnamed bank in Ukraine. These thefts all required the subsequent laundering of stolen funds, reflecting how anti-money laundering practices, cybersecurity, technology, and the international financial system converge.

8.6 Alpha Bay, Hansa, and Operation Bayonet: 2017

In the summer of 2017, Alpha Bay and Hansa, two of the world's largest dark web bazaars estimated to have generated more than a billion dollars in sales of drugs, stolen data, and other illegal goods in just a 3-year period, were taken down in a multinational sting called Operation Bayonet. Although customers on dark web sites are encouraged to encrypt their addresses so that only the seller of product can read it, many do not. These, or other sloppy online hygiene practices, are what create a digital footprint that ultimately helps law enforcement trace activity. In this case, the Alpha Bay administrator's personal e-mail was used in welcome message to new users, which led investigators to his PayPal account, front company, and ultimately his home (Greenberg 2017). Although the takedown threw the darknet participants into chaos momentarily, as in the 2014 Operation Onymous, many other sites remained online including Dream Market, Crypto Market, Ramp, Tochka, Trade Route, and Silk Road, all happily taking on the additional business.

8.6.1 Research challenges

Unfortunately, criminals and their associates do not share information about their methods or successes. Some cybersecurity firms focus on the collection of information from dark web sites and forums to better understand cybersecurity threats, but the maintenance of a low profile is critical to their success, thus making this a difficult area to research. One such firm followed dark web conversations on popular underground forums where specific tools and ransomware attacks against hospitals were discussed, mentioning the many systems that could be targeted, many in the medical industry. It is impossible to know who posted it, and it is not evidence that people who participated in the thread

were responsible. However, this type of information provides insight into hackers' expertise and what future attacks might look like, which may ultimately help companies, law enforcement, and users defend against hacks.

8.7 Challenges and opportunities

While the body of research around money laundering and successful prosecutions is robust, the methods used to obscure and move illicit proceeds through black markets as well as the legitimate financial system are constantly shifting. Given the inherently anonymous nature of the online activities and limited number of firms engaged in this space, the data associated with underground or black markets today are limited. With that said, we know that the nexus between cybercrimes, black markets, and money laundering will continue to grow. The major challenge that anti-money laundering, cybersecurity professionals, and law enforcement face today is around whether the ability to hack, attack, or launder will outpace the ability to defend. Combating threats will require a collaborative approach from both the public and private sectors.

As more consumers shop and pay with connected devices, and commerce increasingly migrates to digital channels, industries must invest in new standards, technologies, and products. One of the best defenses is removing sensitive account data from the payment environment, putting it into a form that cannot be used by criminals for fraud. Products, services, and online platforms should develop built-in security and privacy features, thereby protecting both the product and the customer information from being hacked.

Although transnational organized criminal networks now operate in a new technological paradigm where old rules for combating the criminal element no longer apply, the human factor remains an important component in both executing and detecting crime. In other words, computers, robots, or malicious software is not wholly responsible for all illicit transfers. Conversely, automated systems that monitor transactions can only go so far. There is a limit to how much a machine can catch, and human intelligence remains crucial for developing methods to detect illicit activity. Nascent security and cyber risk management practices within organizations present challenges in fighting criminal actors. A simple step to create stronger defenses is the establishment of robust cybersecurity risk management programs within the private sector that closely intersect (but not necessarily merge) with financial crimes departments. No single person, department, or company has all the skills and resources needed to address these issues, so collaborative practices will be paramount to combating the threat. The anti-money laundering regulatory regime requires that institutions subject to the BSA implement systems and methods to gather certain client and transactional information and continually develop ways to detect and analyze unusual online behaviors. Criminal actors today are adapting to new technologies at rapid pace and seek out the path of least resistance. The lines between fraud, cybercrime, and the laundering of illicit proceeds will continue to blur. Thus, the division between anti-money laundering compliance and cybersecurity risk management professionals is narrowing. To effectively counter cyberattacks and cybercrimes, it is increasingly important that both anti-money laundering and cyber risk professionals in the public and private sectors proactively identify ways to integrate their functions by leveraging and sharing investigative information and monitoring and reporting tools. Regular collaboration and effective communication between financial crimes and cyberdepartments may equip financial institutions with an enhanced ability to refine detective methods, appropriately report suspicious activity to the government, and uncover data-driven solutions.

A well-defined culture of cyber risk awareness and compliance among all members of the public and private sector through annual trainings, information security programs, and governance frameworks will help protect the financial ecosystem, a critical component of our security infrastructure.

References

Ablon, L., Golay, A. A., Libicki, M. C. M*arkets for Cybercrime Tools and Stolen Data: Hacker's Bazaar*. Santa Monica, CA: RAND Corporation. pp. 4, 5, 8. (2014). Available at: https://www.rand.org/content/dam/rand/pubs/research_reports/RR600/RR610/RAND_RR610.pdf.

Cetera, M. *Prices Rise for Your Data on the Black Market.* (2016, May 3). Accessed June 17, 2017. Available at: http://www.bankrate.com/financing/credit-cards/prices-rise-for-your-data-on-the-black-market/.

Coinmarketcap.com. CryptoCurrency market capitalizations. Available at: https://coinmarketcap.com/.

Egmont Group. *The Egmont Group of Financial Intelligence Units.* Toronto: Egmont Group. (2018). Available at: http://www.egmontgroup.org.

FBI (Federal Bureau of Investigation). *Dozens of Online "Dark Markets" Seized Pursuant to Forfeiture Complaint Filed in Manhattan Federal Court in Conjunction with the Arrest of the Operator of Silk Road 2.0*. Washington, DC: FBI. (2014, November 7). Available at: https://www.fbi.gov/contact-us/field-offices/newyork/news/press-releases/dozens-of-online-dark-markets-seized-pursuant-to-forfeiture-complaint-filed-in-manhattan-federal-court-in-conjunction-with-the-arrest-of-the-operator-of-silk-road-2.0.

FDIC (Federal Deposit Insurance Corporation). *Guidance for Financial Institutions on Reporting Computer-Related Crimes*. FDIC Financial Institution Letter FIL-124-97. Washington, DC: FDIC. (1997, December 5). Available at: https://www.fdic.gov/news/news/financial/1997/fil97124.html.

FFIEC (Federal Financial Institutions Examination Council). *Cybersecurity Assessment Tool*. Arlington, VA: FFIEC. Page last modified: September 1, 2017. Available at: https://www.ffiec.gov/cyberassessmenttool.htm.

FinCEN (Financial Crimes Enforcement Network) *Advisory to Financial Institutions on E-Mail Compromise Fraud Schemes*. Vienna, VA: FinCEN. (2016a, September 6). Available at: https://www.fincen.gov/sites/default/files/advisory/2016-09-09/FIN-2016-A003.pdf.

FinCEN. *Advisory to Financial Institutions on Cyber-Events and Cyber-Enabled Crime*. Vienna, VA: FinCEN. (2016b, October 25). Available at: https://www.fincen.gov/sites/default/files/advisory/2016-10-25/Cyber%20Threats%20Advisory%20-%20FINAL%20508_2.pdf.

Fox-Brewster, T. Crooks behind $81M Bangladesh Bank heist linked to Sony Pictures hackers. *Forbes*. (2016, May 13). Available at: https://www.forbes.com/sites/thomasbrewster/2016/05/13/81m-bangladesh-bank-hackers-sony-pictures-breach/#6a0de2142ee6.

FRB (Federal Reserve Bank). *Agencies Issue Advanced Notice of Proposed Rulemaking on Enhanced Cyber Risk Management Standards*. Washington, DC: FRB. (2016a, October 19). Available at: https://www.federalreserve.gov/newsevents/pressreleases/bcreg20161019a.htm.

FRB. *Guidance Concerning Reporting of Computer Related Crimes by Financial Institutions*. FRB Supervisory Letter SR 97-28. Washington, DC: FRB. (2016b, April 21). Available at: https://www.federalreserve.gov/supervisionreg/srletters/sr1609.pdf.

Greenberg, A. Dark wallet is about to make Bitcoin money laundering easier than ever. *Wired*. (2014, April 29). Available at: https://www.wired.com/2014/04/dark-wallet/.

Greenberg, A. Global police spring a trap on thousands of dark web users. *Wired*. (2017, July 20). Available at: https://www.wired.com/story/alphabay-hansa-takedown-dark-web-trap/.

Greene, C., Stinebower, C. N., and Wolff, E. D. FinCEN cybercrime advisory expands SAR requirements. *Law360.* (2016, November 29). Available at: https://www.law360.com/articles/864549/fincen-cybercrime-advisory-expands-sar-requirements.

Gup, B. E. *Money Laundering, Financing Terrorism and Suspicious Activities.* New York: Nova Science Publishers. p. 8. (2007).

IRS (Internal Revenue Service). *Bank Secrecy Act*. Washington, DC: IRS. Page last modified: August 6, 2017. Available at: https://www.irs.gov/businesses/small-businesses-self-employed/bank-secrecy-act.

NCUA (National Credit Union Administration). *Guidance for Reporting Computer-Related Crimes*. NCUA Regulatory Alert 97-RA-12. Alexandria, VA: NCUA. (1997, December 5). Available at: https://www.ncua.gov/Resources/Documents/97-RA-12.pdf.

NYDFS (New York Department of Financial Services). *Regulation Emphasizes Compliance Culture at Top Levels of the Institution*. Albany, NY: NYDFS. (2017, February 16). Available at: http://www.dfs.ny.gov/about/press/pr1702161.htm.

Office of the Comptroller of the Currency. *Bank Secrecy Act: Combating Money Laundering and Terrorist Financing*. Washington, DC: Office of the Comptroller of the Currency, US Treasury Department. Available at: https://www.occ.treas.gov/topics/compliance-bsa/bsa/index-bsa.html.

PwC. Global Economic Crime Survey. PwC. (2018). Available at: https://www.pwc.com/gx/en/services/advisory/forensics/economic-crime-survey/cybercrime.html.

Richet, J.-L. Laundering money online: An overview. *Harvard Law Blog* (2015, February 7). Available at: http://blogs.harvard.edu/jeanlouprichet/files/2015/02/Laundering-Money-Online_an-Overview.pdf.

Sharman, J. C. The Money Laundry: Regulating Criminal Finance in the Global Economy. Ithica, NY: Cornell University Press. pp. 14–16. (2011).

UNODC (United National Office on Drugs and Crime). *Estimating Illicit Financial Flows Resulting from Drug Trafficking and Other Transnational Organized Crime*. Vienna: UNODC. pp. 5, 39. (2011, October). Available at: https://www.unodc.org/documents/data-and-analysis/Studies/Illicit_financial_flows_2011_web.pdf.

US Treasury Department. *History of Anti-Money Laundering Laws*. Washington, DC: US Treasury Department. Available at: https://www.fincen.gov/history-anti-money-laundering-laws.