The Convergence of Cyber, Fraud, and AML

How the Puzzle Pieces Fit Together to Solve the Emerging Cyber Risk

Kevin W. Toth, CAMS

Contents

Executive Summary

During Berkshire Hathaway's annual shareholder's conference in 2017, Warren Buffett opined that "cyberattacks pose a bigger threat to our existence than nuclear weapons" (Oyedele, 2017). Industry analysis estimates "cybercrime damages will cost the world $6 trillion annually by 2021," which represents the greatest transfer of economic wealth in history and will be more profitable than the global drug trade (Morgan, 2018). IBM's chairman, president, and CEO stated that "cybercrime is the greatest threat to every company in the world" (Morgan, 2018). From a macro-level perspective, cybercrime is the greatest emerging threat our government and economy now face. From an individual perspective, not a day goes by without news of personally identifiable information being compromised from data breaches at retailers or other entities (e.g., Target, Home Depot, Office of Personnel Management).

It is abundantly clear that cybercrime affects everyone at a macro and micro level, both professionally and personally. What is not so clear is how the continuing emergence of cybercrime impacts a financial institution from a tactical, organizational, and compliance perspective. Financial institutions are historically siloed, and cybercrime is unique in that it transcends three traditionally separate functions: Cyber, Fraud, and Anti–Money Laundering (AML). How do financial institutions cohesively respond to the emerging cyber threat on an enterprise-wide basis while still maintaining full adherence to Anti-Money Laundering / Banking Security Act (AML/BSA) reporting? The proposal this white paper suggests is the Fusion Cell approach, which is a specialized task-force within the financial institution that is best equipped to handle the cyber threat. The Fusion Cell takes a risk-based approach in converging expertise in Cyber, Fraud, and AML to appropriately respond to all cyber events and to fulfill growing and expanding regulatory expectations.

Because cybercrime is the number one risk the AML community is challenged with, it is essential that all AML professionals understand how the convergence of Cyber, Fraud, and AML occurs. It is no longer sufficient for the AML professional to be a subject matter expert (SME) in traditional money laundering typologies and red flags, but rather it is vital that AML teams have a working knowledge of how cybercrime and fraud impacts (and is intertwined with) their investigations. To that end, the first part of this white paper will focus on foundational concepts, terms, and typologies needed to understand cybercrime.

Cyber Event vs. Cyber-Enabled Crime

The term cybercrime needs to be defined and the nuanced differentiation of its various forms explained. There is no universally accepted definition of *cybercrime*, however it is generally defined as a criminal action that is conducted by or through the use of a computer or the Internet (Meeuwisse, 2015-2017). While cybercrime is the umbrella term, it can be further differentiated between a cyber event and a cyber-enabled crime. A cyber event is an act that compromises a computer system by gaining unauthorized access via various methods (e.g., phishing, credential stuffing, banking Trojans, etc.). A cyber-enabled crime is an illegal action that is carried out or

facilitated by electronic systems and devices, such as fraud, drug dealing, child pornography, weapons trafficking, etc. (Advisory, 2016). At times, these two categories are independent of each other. For example, a cyber event can occur when an individual gains access to a website and essentially shuts it down (i.e., a distributed denial-of-service attack), however, no other crime is committed. A cyber-enabled crime can occur without being preceded by a cyber event, for example: pedophiles sharing child pornography online. Although cyber events and cyber-enabled crimes can occur in isolation, they are usually not mutually exclusive and are typically intertwined in some capacity. For example, an individual creates a banking Trojan to access a customer's bank account (a cyber event) and to then fraudulently withdraw money, which is laundered through the financial system (cyber-enabled crimes). Later in this paper, specific typologies and case studies of how cyber events and cyber-enabled crimes are intertwined will be discussed.

> "ESTIMATED GLOBAL REVENUE FROM CYBERCRIME: $1.5 TRILLION+ ANNUALLY" (MCGUIRE, 2015).

Cyber Environment

Contrary to stereotypes, the responsible parties behind cyber events are not lonely individuals living in their parents' basement. The entity that is culpable for conducting a cyber event is defined as a threat actor, and they run the gamut from highly educated individuals to organized crime syndicates to nation-states. According to the Harvard Business Review, the public should disregard their stereotypes and think of threat actors as "sophisticated, professional operations working out of an office tower" (Gardiner, 2017). There are numerous studies exemplifying that cybercrime "now has its own economy…that not only mirrors its legitimate counterpart but that both feeds off it and feeds into it" (McGuire, 2015). In terms of nation-states, there is evidence that Lazarus (a notorious group of North Korean hackers) was behind a global rash of cyberattacks on financial institutions in which stolen funds were ultimately laundered to support North Korean nuclear weapons development (Alcantar, 2017). Over the past few years, other countries such as Iran and Russia have been accused of launching (directly or indirectly) cyber events against adversaries for either financial and/or political gain (e.g., shutting down websites of major financial institutions of political opponents). On an individual level, only unsophisticated criminals physically rob a bank nowadays. Why risk physical identification, harm, and/or capture when you can conduct the same activity electronically (and safely), behind a computer screen potentially thousands of miles away? Studies have shown that the "earnings of individual cybercriminals…exceed their counterparts in the traditional crime world" by a magnitude of 10–15% (McGuire, 2015). Nowadays, all sorts of criminals have turned 'cyber' and, thus, the environment has become much more complex.

> "THERE IS EVIDENCE THAT CYBERCRIME REVENUES OFTEN EXCEED THOSE OF LEGITIMATE COMPANIES" (MCGUIRE, 2015).

Going Deep, Deeper, Dark

A contextual understanding of the environment in which threat actors operate is the next foundational piece required for the AML professional. Threat actors operate in all three layers of the Internet, the clear/surface web, the deep web, and the dark web. What differentiates these three layers? The best explanation is visual: the classic picture of the iceberg showing critical mass under water

Credit: (dragonzz, 2018)

As you can see, a vast majority of the information available on the Internet is only accessible on the deep and/or dark web. The deep web is defined as Internet content that cannot be seen and is not indexable by search engines (Meeuwisse, 2015-2017). Material found in the deep web is usually innocuous and not of a concern, as most databases or intranet sites that require a password for access are considered the deep web (e.g., a hospital's medical records or a financial institution's transactional database). As a financial crime professional, we are much more concerned about the dark web which is a subset of the deep web. The dark web is defined as a network of websites that are publicly accessible (if you know how to find them, as they are not registered on standard search engines) but hide their server locations making it extremely difficult to track who is behind the website, who is accessing the information, and the context within the dark web website (Meeuwisse, 2015-2017). The most common software used to access the dark web is TOR, which is a platform that anonymizes communication and a person's identity. It does so by bouncing a person's IP address and subsequent communications across multiple relays to hide their exact location and identity. The dark web is clearly an environment where money launderers, terrorist financiers, and organized crime syndicates can and do thrive.

Attack Vectors/Fraud Typologies

Now that the “where” is defined, let’s discuss the “how.” Attack vectors are the methods that threat actors employ to achieve their malicious goals, or said in another way, attack vectors

BETWEEN MAY 2013 AND MAY 2018, THERE WAS A 136% INCREASE IN BEC ATTACKS WITH TOTAL LOSSES OVER $12 BILLION (BUSINESS E-MAIL COMPROMISE, 2017).

are the methods in which criminals fraudulently gain information and/or money (Meeuwisse, 2015-2017). Let's be clear that information in this space is a lucrative asset worth as much or more than the actual crime of taking money directly. Like most criminal operations, the sophistication and speed in which cyber threats occur is constantly increasing.

Phishing

One of the most persistent attack vectors utilized today is phishing, where a threat actor utilizes e-mails, websites, apps, and phone calls to get an unsuspecting individual to give up compromising information (or to gain access to their information). For example, a victim is tricked into clicking a link or attachment that installs malicious software onto their computer to gain access to sensitive information (e.g., financial data or log-in credentials). Many times this is conducted by spoofing, which is "concealing the true source of electronic information by impersonation or by other means" (Meeuwisse, 2015-2017). A threat actor can create a website which mirrors that of a financial institution's webpage with a similar URL, but is a facade. Once the victim enters in their log-in credentials, the malware then compromises personally identifiable information.

Case Study

In 2013, the massive Target data breach occurred, which is a great example of a phishing attack. While full details have not been disclosed, it is widely accepted that threat actors gained access to the Target point-of-sale (POS) systems from a contractor that Target employed. Specifically, hackers obtained the log-in credentials of the contractor's employee through a phishing campaign. Once the threat actors gained access to the contractor's system, the criminals placed malware on Target's POS system, stole credit card information from over 70

Business E-Mail Compromise

Business E-mail Compromise (most commonly referred to as BEC, or CEO impersonation), is "defined as a sophisticated scam targeting businesses working with foreign suppliers and/or businesses who regularly perform wire transfer payments" (2016 Internet Crime Report, 2017). The first step in BEC is when threat actors (usually organized crime syndicates) will target U.S. businesses with the initial goal of collecting as much information about the company and its executives (e.g., CEO) as possible. The threat actors will then gain access to the e-mail system of the CEO (or a similar high-level executive) via the spear-phishing attack vector (a more concentrated version of phishing). When the CEO is travelling or in all-day meetings, the threat actor will send an e-mail from the CEO's account to an employee who works in the finance department, instructing them to send an immediate wire to a trusted vendor. Even though the vendor is known to the finance employee, the beneficiary's account number provided in the instructions "by the CEO" are slightly different from the normal bank account wires are normally

remitted. This account is usually a pass-through account set-up by the criminal organization (or a myriad of mule or shell company accounts). Once the wire is remitted, the funds quickly become untraceable as they are layered throughout several accounts and counties, and ultimately end up in the criminal's hands.

The FBI has found that Asian banks in China and Hong Kong remain the primary destination of these funds (Business E-mail Compromise, 2017). Per the FBI Internet Crimes Complaint Center (IC3), "the BEC scam continues to grow, evolve, and target businesses of all sizes" (Business E-Mail Compromise, 2017).

Banking Trojans

An attack vector that is much harder for companies to detect is a banking Trojan, as it targets individual customers instead of financial institutions. A Trojan is software that appears to be harmless but hides and facilitates malicious applications within the software package (Meeuwisse, 2015-2017). The most common method Trojans deploy is through cell phone applications that appear to be legitimate. As an individual is downloading this 'legitimate' application, malware is being installed that allows the threat actors access to personally identifiable information. According to some estimates, more than 90% of developers who create banking Trojans reside in Eastern Europe or Russia (2016 Internet Crime Report, 2017). For a financial institution (or any other company), this is much harder to detect as the individual customer is compromised, not the business infrastructure itself.

Ransomware

Another Trojan that is becoming more ubiquitous is ransomware. This is a malware usually disguised as a legitimate file and once a user decides to open it, the malicious software starts installing. Once the malware is installed on the computer, it will block all functionality of the computer (or system) until a ransom is paid, usually via cryptocurrency. Although this can be a financial liability and a moderate annoyance to an individual, the effects of a systematic ransomware attack on a large corporation can be enormous, depending on the number of users affected, loss of production, and the amount of ransom required to regain access (Meeuwisse, 2015-2017).

ATM Jackpotting

An attack vector that is not as prevalent but is an emerging threat is ATM jackpotting (also named the ATM cash-out scheme). There are two ways that ATM jackpotting occurs. The first is when an ATM is physically broken into (i.e., by utilizing a universal key to open the ATM to remove the hard drive), after which malware is installed. The malware will then fraudulently dispense cash from the ATM when designated by the criminal for a money mule to retrieve. The second method occurs when malware is installed in the bank's central operating system. Once this happens, the malware artificially inflates individual account balances, and cybercriminals will initiate cash withdrawals via the ATM network. Although ATMs are limited in funds they can

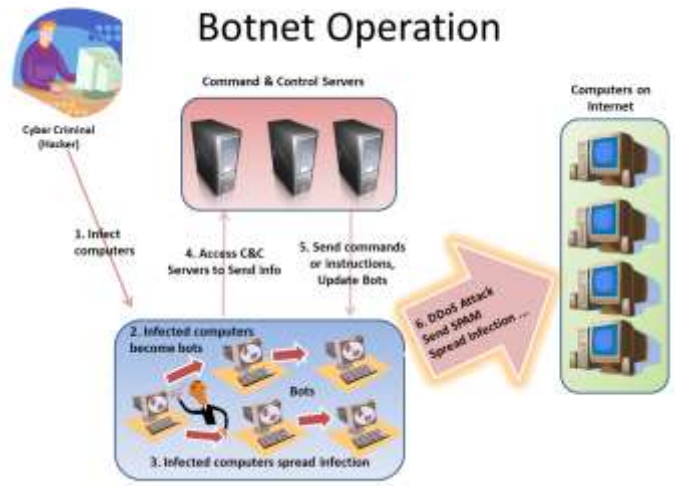
dispense at any given time, the exploitation of hundreds of ATMs coupled with the utilization of countless money mules can reap millions of dollars in a single day (Heinzman, 2018).

Man-in-the-Middle (MITM) Attacks

MITM attacks are also another way threat actors can gain access to information and data. Although complex in its technical aspects, the basic goal of a MITM attack is to intercept communication between two parties. As a theoretical example, assume Bob wants to send money to Cyndi, and they are communicating on a trusted platform. Once Cyndi instructs Bob on where to remit the funds (by providing an account number or e-mail address), the money is typically sent by Bob and received by Cyndi. However, in the MITM scheme, the threat actor (named Peter) will intercept communications between the parties. Instead of Bob thinking he is directly communicating with Cyndi (and vice versa), they are both in fact communicating with Peter. Peter will then provide Bob with another account number (or e-mail address), and thus the funds are ultimately sent to Peter instead of Cyndi.

Botnet

Although not an attack vector itself, the term *botnet* will be introduced as it is an essential component of the next attack vector that will be described. Traditionally, a "bot" is a malware that allows the threat actor to take control over an affected computer. A botnet is simply that, a network of bots. A more detailed definition of a botnet is a connected set of programs designed to operate together over a network to achieve specific purposes (Meeuwisse, 2015-2017). Under the auspice of how they are used by criminals with bad intentions: A botnet is a group of private computers that are infected with malware and are under the control of a threat actor, without the owner's awareness (Meeuwisse, 2015-2017). Botnets are an efficient and cost-effective way to gain computing and processing power to enable cybercrimes. If you are the head of an international criminal syndicate and want to engage in cyber-related activity, you can either build servers from scratch, or simply build malware to harness the power of a private citizen's personal laptops, cell phones, and tablets (the Internet of things) as part of a botnet. Which option would you choose, especially if the person whose device is affected has no idea they are part of the botnet? The only indicator that a device has been compromised is the utilization of many more CPU's (central processing units) than the device would normally use (above visual is sourced from Alexander, 2013).



Credential Stuffing

According to the *2018 Verizon Data Breach Investigations Report*, the credential stuffing attack vector is one of the most prevalent today (2018). The use of stolen identities from third-party data breaches to fraudulently gain access to other accounts is called *credential stuffing* (Townsend, 2017). With this attack vector, botnets are heavily utilized as they fulfill a key requirement within the process. To exemplify credential stuffing, a hacker employs a successful spear-phishing attack against employees in a company, and the hacker gains access to that company's systems. Once inside, the hacker will collect sensitive information (i.e., log-in credentials, e-mail addresses) and extract it out of the company's systems. The hacker will usually sell these compromised credentials in bulk on the dark web.

A threat actor (e.g., international crime syndicate) will then purchase the credentials with the ultimate goal of obtaining access to individual accounts with other companies/websites. For example, if a threat actor has a username and password combination that was hacked from Company A; they will use that same e-mail and password combination (with the help of a credential stuffing tool) at websites for Company B, Company C, Company D, etc., to see what authenticates. Botnets are then deployed for maximum effectiveness. These tools are usually available for purchase/rental in the dark web, and one of the most common is SentryMBA, partly because this particular tool is free and easy to use (Townsend, 2017). For example, if suzyq@gmail.com with the password of "123456" was compromised from Bank A, the threat actor will feed the e-mail and password combination into SentryMBA, which will then test that e-mail and password into Bank B's website (and Bank C's, and Bank D's, etc.) via the botnet. If these attempts succeed (which frequently they do, because many people use the same username/password combination across multiple websites), the threat actor then has access to account balances, reward points, and other personally identifiable information (names, address, phone numbers, etc.). The threat actor will then either drain the account and launder the money

or will sell the account information (for a price reflective of the balance) on the dark web to monetize the data (above images are sourced from Criminals Are Using, 2017).

While the above attack vectors are the most commonly used, this is by no means an extensive list. The landscape continuously evolves as technology changes and as the gap between cybercriminals and law enforcement ebbs and flows. Now that the understanding the overall cyber environment is in place, including the threat actors and the various methods they employ to conduct cyberattacks, the next piece of the puzzle is to dive into the deep web and some of its inner workings. This is where much of the 'action' takes place; knowing about it will help provide an understanding about how the convergence of Cyber, Fraud, and AML occurs.

ILLICIT ONLINE MARKETPLACES HAVE MINIMUM ANNUAL GLOBAL REVENUES OF $860 BILLION (MCGUIRE, 2015).

Dark Web Inner Workings

As mentioned above, the dark web consists of websites that hide their server locations and require certain authorization and/or software for access (Meeuwisse, 2015-2017). The dark web is part of the deep web but requires the correct software (e.g., Tor) and a known dark web address for access. Obtaining the dark web address is not as easy as the clear web, as many sites only grant access by word of mouth or on ratings based on status and trust (McGuire, 2015). It is aptly named as almost all information, products, and services on the dark web are of an illegal nature, otherwise, they would be sold on the clear web. The dark web provides a safer space for nefarious activity to occur. After all, why risk arrest by buying drugs on a street corner when you can buy drugs online via the dark web, get them discreetly shipped to your house, and even access product and seller reviews?

The Dark Web Market

Before we get into the various types of products and services that are for sale, we must understand how they are sold. “There are, at present, two types of marketplaces found on the dark web: cryptomarkets and vendor shops. Cryptomarkets bring together multiple sellers (known as vendors) that are managed by administrators in return for a commission on sales" (Paoli et al., 2017). Think of a cryptomarket as the dark web Amazon; instead of buying everyday household items, you can buy illicit goods and services. Cryptomarkets have some of the same protections as an Amazon-type marketplace does; for example, they offer payment protection to customers as funds are only released to the vendor once the customer receives their products (Paoli et al., 2017). Cryptomarkets also provide third party adjudication services and posts reviews of individual vendors (Paoli et al., 2017). On the other hand, "vendor shops, also known as 'single-vendor markets,' are set up by a vendor to host sales for that vendor alone" (Paoli et al., 2017). You can buy whatever illicit goods or services directly from the vendor, and most do not charge a commission.

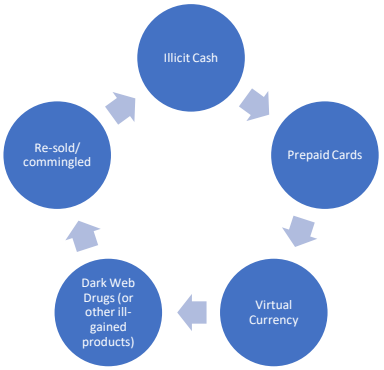
The Silk Road was the first true dark web marketplace and was considerably the most notorious cryptomarket at the time. Although that website was shut down by federal authorities in 2013, it was estimated to have brought in over $7 million in revenue on a monthly basis

(Kruithof et al., 2016). What can you buy from a cryptomarket or vendor shop on the dark web? You name the product or service, you can buy it. Although drugs account for 57% of listings on the dark web, you can also buy chemicals, counterfeit items, stolen financial information, weapons (of any kind), assassins, sex slaves, and child pornography, to name a few (Kruithof et al., 2016). According to the DEA, Carfentanil (a fentanyl-related compound) is the most potent commercial opioid used and is primarily bought via illicit networks and dark web purchases (DEA Strategic Intelligence, 2017). The dark web drug trade has shown to be resilient to law enforcement, as drug-related revenue has doubled, the number of transactions has tripled, and the number of drug listings has increased 5.5 times over a three-year period (Kruithof et al., 2016). Research has also indicated that drug-related purchases on the dark web are made by both individual users and by drug-trafficking organizations intending to buy wholesale for offline distribution (Kruithof et al., 2016). As mentioned, drugs are the most common product bought, but they are not the only product by far. Below are screenshots of a cryptomarket and a vendor shop selling a variety of items:

Top two images: (Kruithof et al., 2016)

Bottom image: (The Ultimate Guide, 2013)

No matter what type of illicit product or service is being bought on the dark web, it must be paid for, same as everyday clear web purchases. Unlike processing a credit card payment for an Amazon purchase, most "criminals who work in the shadows of the dark web are often paid for in virtual currency, which is an attractive way to launder funds" (Khan, 2016). This is probably not surprising to most, as the relative anonymity and the rapid nature of virtual currency is extremely attractive, much more so than fiat currency or other electronic means (e.g., credit card or ACH payments). For example, a criminal can load multiple prepaid credit cards with illicit cash and buy virtual currency (e.g., bitcoin). Those bitcoins are then used to purchase illicit drugs on the dark web, which are then resold on the streets and commingled with clean funds (Khan, 2016).



As mentioned, virtual currency can be perceived as an anonymous form of payment, but is not completely free of identity tracing. Law enforcement and regulators are trying to force more transparency in this new form of payment; however, other actors are developing tools to make virtual currency more anonymous. Specifically, one piece of software being used is the Dark Wallet, which is "a bitcoin application designed to protect its user's identities far more strongly than the partial privacy protections bitcoin offers in its current form. It could neuter impending bitcoin regulations that seek to tie individuals' identities to bitcoin ownership" (Greenberg, 2014). In an interview with *Wired* magazine, the developers of the Dark Wallet said they created it as a "private means for black market transactions," and that the application is "simply money laundering software" (Greenberg, 2014). Blogs have sprouted up all over the Internet on how to utilize the Dark Wallet (and similar applications), showing how one could send millions of dollars' worth of bitcoin from the United States and other countries right to the pockets of the mujahedeen (Copestake, 2014). It is obviously concerning that the use of virtual currency and the furtherance of software like the Dark Wallet allows criminals to utilize the dark web to continue to buy illicit goods and services (Copestake, 2014).

Putting the Puzzle Pieces Together

The last major piece to this puzzle, and the glue that puts everything together, is to exemplify how money laundering fits into the equation. At the end of the day, criminals who utilize the cyber environment to commit fraud ultimately need to monetize that information and launder the proceeds so that the funds appear legitimate. The job of an AML professional is hard enough, as untangling complex layering schemes and identifying beneficial owners is par for the course. The cyber world adds an additional web of complexity as anonymity is layered directly on top of anonymity (i.e., the dark web, virtual currency, Dark Wallet). The nefarious cyber world makes masking identities and motives that much more removed from plain sight. Additionally, the number of AML subject matter experts who have a deep enough understanding to truly comprehend what is occurring in this space adds yet another layer of complexity to the issue.

Understanding the convergence of Cyber, Fraud, and AML is of utmost importance in today's compliance and regulatory landscape.

Theoretical Case Study

To help glue the pieces of the puzzle together, the exemplification of the convergence of Cyber, Fraud, and AML via a theoretical case study will be presented. Let's say a hacker (named "Henry Hacker") targets a major retailer and breaches its firewall and security systems. Henry Hacker will then access account-level information, specifically targeting login credentials for the retailer's customers (e.g., usernames, passwords, associated e-mail addresses, etc.). Henry Hacker will then extract that information out of the retailer's website and move it to the dark web. Depending on the motive and ideology of Henry Hacker, he will either dump the stolen information into the dark web for free, or more usually, he will post it for sale.

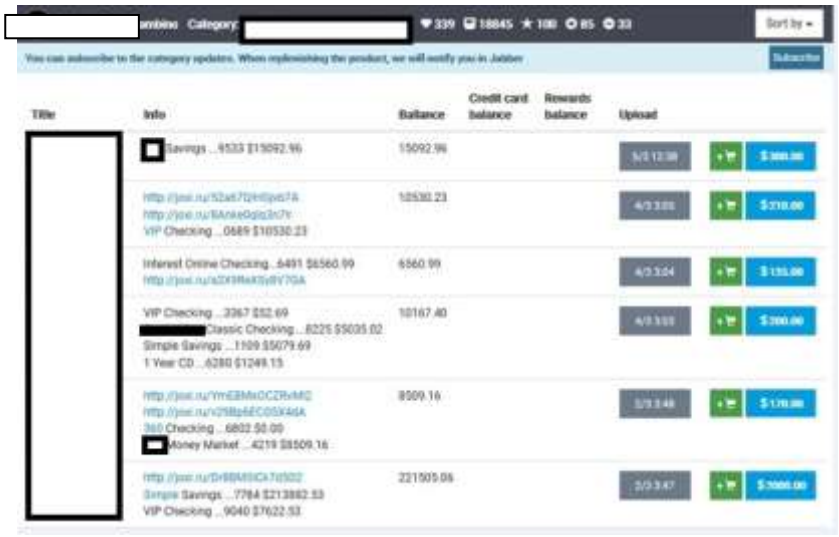
"THE COST TO ACQUIRE SOCIAL SECURITY INFORMATION, DATE OF BIRTH, RESIDENTIAL ADDRESSES: $3.00" (MCGUIRE, 2015).

The next player in our scenario is Carlos Cybercriminal. As stated earlier, do not think of Carlos as a lonely person sitting in his parents' basement, but as an account executive at a reputable sales firm who is also a representative of a global, sophisticated criminal organization in his "off-hours." Once the stolen information is on the dark web, Carlos Cybercriminal will then pay Henry Hacker for this stolen information via cryptocurrency. After the transaction occurs, Carlos will now have the stolen usernames, passwords, and associated e-mail addresses of the retailer's customers in his possession. The next step for Carlos is to buy or develop an online tool that efficiently exploits the stolen information via a botnet to conduct a credential stuffing campaign that targets a financial institution. As a reminder, Carlos has the usernames, passwords, and e-mail addresses of customers from a major retailer and will try to use those same username and password combinations (from the retailer) to log into the financial institution's website. How can this happen and how can this approach be successful? Think about the usernames and passwords you enter for every website and/or system you interact with, and one can bet that the same combination is utilized for more than one account.

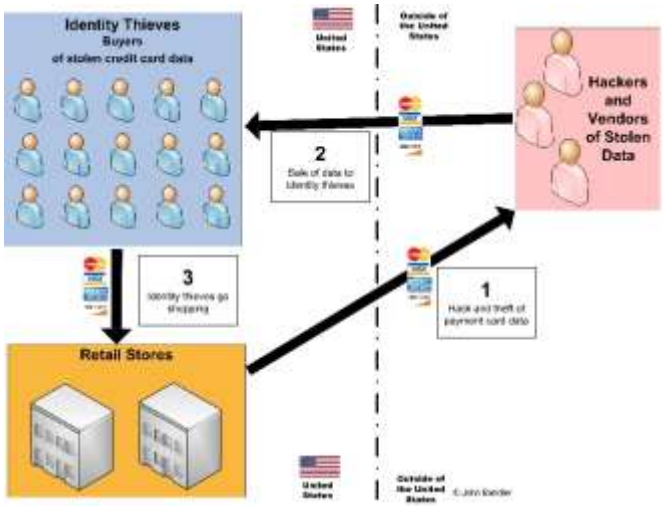
Now that we know why this can happen, the next step is to exemplify how it occurs. Carlos Cybercriminal will take the thousands (or millions) of username and password combinations and put them into a credential checking tool (e.g., SentryMBA) that enables users to target specific companies. These tools are utilized across a botnet to maximize the brute force of thousands of computers assigned to the same task. When the botnet

ACCORDING TO ONE STUDY, 81% OF AMERICANS USE THE SAME PASSWORD FOR MORE THAN ONE SITE, AND 92% OF MILLENNIALS USE THE SAME PASSWORD ACROSS MULTIPLE ACCOUNTS (SURVEY, 2017).

confirms that a specific username and password will access an account on the financial institution's website, Carlos Cybercriminal will log into the compromised e-mail to satisfy multi-factor authentication requirements. Now, the criminal is in and has full control of the bank account. Specifically, Carlos Cybercriminal can access a variety of information including but not limited to: name, account type, account balance, credit limit, rewards tier and balance, phone numbers, additional e-mail addresses, physical addresses, etc. Carlos Cybercriminal can either cash out of the account using various conduits (detailed in the next section), or can sell the account for a price reflective of the balance. Usually, the higher the balance/available credit (and/or the higher the amount of accrued rewards points), the higher the selling price on the dark web. For example, the "sale of personal information on just (high-valued) 50 credit or debit cards can generate earnings of $250,000–$1 million" (McGuire, 2015). Below is a screenshot of a dark web vendor shop that is selling various retail bank accounts acquired through a credential stuffing campaign (with some information redacted):



Individuals and/or entities that usually buy these compromised accounts are identity thieves who will utilize the account to fraudulently make purchases or exploit the money some other way. Carlos Cybercriminal will usually ask for cryptocurrency deposits, wire transfers, or money orders as payment.



(Bandler, 2017).

Laundering the Cybercrime Proceeds

Criminals who operate in the cyber space are sophisticated and well-educated, which means that the methods utilized to launder the funds are complex as they try to stay ahead of AML professionals and law enforcement (Cybercrime and Money Laundering, 2014). As such, there are countless methods for how the laundering can occur, but below are the main conduits that cybercriminals use to clean their funds.

Money Mules

One of the primary and consistently used conduits is the utilization of money mules. A money mule is a witting or unwitting person who receives, and then transmits illegally acquired funds (Bandler, 2017). Witting money mules are individuals who knowingly are hired to accept dirty cash, keep a portion as commission, and then quickly transfer that money abroad, traditionally via wire transfer (or other conduits). An unwitting money mule is an individual whose accounts are utilized in the same fashion, albeit with the difference that they do not know the funds coming in and out of the account are proceeds from crime. How are they recruited, you might ask? These individuals usually fall victim to a scam, such as applying for a "work from home position," a romance scam, or at times, other compromised accounts are utilized to layer the funds. Money mules are usually disposable and are used once (or a minimal amount of times). One of the best ways financial institutions can track and identify mules is via the National Cyber Forensic Training Alliance's (NCFTA) money mule database. If a financial institution is not part of NCFTA and not utilizing this database, they should consider doing so. It is a give-data-to-get-data environment, whereas participating members need to actively participate and share data for reciprocation to occur (Swecker, 2016).

"95% OF MONEY MULE ACTIVITY HAS LINKS TO CYBERCRIME ACTIVITIES" (MCGUIRE).

Shell Companies

Shell companies offer a more permanent (and/or developed) and complex infrastructure to serve as a conduit to launder cybercrime proceeds. Even with the recent regulations in the United States surrounding beneficial ownership identification, shell companies are still a popular method for cybercriminals. Shell companies offer a deeper layer of anonymity and can be used multiple times, even if more effort and time are required to initially set them up. Therefore, shell companies are very attractive to cybercriminals.

Wire Transfers

Another major conduit that criminals utilize to launder cybercrime proceeds are wire transfers, as they are "an essential part of global funds transfer and are essential to the cybercrime economy" (Bandler, 2017). Wire transfers can be initiated or misdirected based on fraud (e.g., business e-mail compromise scheme), are an essential part of cryptocurrency transactions, and are a fast and efficient way to layer funds abroad (Bandler, 2017). It is found through case studies that wires are often used at the beginning of the laundering process to extract money from compromised accounts (Moneyval, 2012).

Money Remittance Services

A very traditional conduit is a money remittance service such as Western Union or MoneyGram (Bandler, 2017). Not only are these services utilized across the globe, but they offer an extent of anonymity as cybercriminals utilize fake conductor and recipient names to move the funds. Money remittance providers are usually inexpensive and at times appear to offer more lax AML compliance programs, which are all attractive features for cybercriminals. According to one study by MONEYVAL[1], "the use of money remittance providers is the most common technique for laundering criminal money derived from cybercrime" (Moneyval, 2012). Both money orders and wire transfers are made in small amounts below the reporting threshold to avoid having to justify their origin (Moneyval, 2012).

Digital Currency

Digital currency is the fifth conduit for how the proceeds of cybercrime are moved. It would be inappropriate and inaccurate to state that much of digital currency in today's economy is dirty money, as there are both legitimate and illegitimate uses of this form of currency. Digital currency is a natural way for cybercriminals and threat actors to exchange value for goods and services as both digital currency and cybercrime is conducted on the same medium—the Internet. Take the street-level form of drug trafficking, where drugs are exchanged for cash. The use of digital currency in this interaction model would be inefficient and impractical. The reverse is true for cybercrime, where the need for an instantaneous and international transfer of funds is required, which makes cash inefficient and impractical (Bandler, 2017). Although person-to-person (P2P) services like Paypal and Venmo are not digital currency platforms, the use of these

[1] MONEYVAL is another name for the Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism.

digital payment systems is increasingly being used for the same reasons and benefits that digital currency provides.

Gaming Currency

One of the newer and most emergent conduits is the utilization of gaming currency. Gaming currency (or video game currency) is generated by players achieving certain levels or completing various tasks within a video game. Although gaming currency is utilized by players within a unique game, certain products allow users to buy and sell gaming currency for fiat currency. Cybercriminals will purchase gaming currency or exploit vulnerabilities within the game to generate gaming currency (without even having to play!), and then will sell that currency to legitimate users. Frequently, cybercriminals are 'carding', or using fraudulent or stolen credit cards to purchase gaming currency. Due to the speed of the Internet, dirty proceeds generated from cybercrime can quickly be converted into gaming currency, which legitimate video game users purchase. Then the cybercriminal will convert the clean proceeds of that transaction into a form of fiat currency, which is then utilized to fund other criminal activities (Abel, 2018).

Transaction Laundering

Although a vast majority of illicit goods and services are bought on the dark web, it does not mean that the clear web is free from crime; in fact, when it comes to the clear web, transaction laundering reigns true (Teicher, 2017). Transaction laundering occurs when a cybercriminal exploits a legitimate payment ecosystem by funneling unknown transactions through e-commerce payment accounts or by setting up fake online shops on the clear web (Teicher, 2017).

Increasingly, this is becoming a popular method of offering illegal goods and services as customers do not have to go through the steps (or understand the steps) to access the dark web and can simply perform these actions right after checking their Facebook account. One-way transaction laundering can occur is when a cybercriminal will pose as a legitimate enterprise and will attempt to partner with a legitimate online reseller with the proposal of sharing operating expenses while using the same payment ecosystem to increase sales for both parties.

THE UTILIZATION OF THE CLEAR WEB TO SELL ILLICIT GOODS AND SERVICES HAS GENERATED OVER $300 BILLION IN GLOBAL SALES (TEICHER, 2017).

Transaction Laundering Examples

Assume you sell coffee products online and allow another company to sell coffee mugs through your website. This would appear to benefit both parties as expenses would be shared. However, the 'coffee mug' company is a front company that sells drugs, and the proceeds from drug sales are commingled through the coffee website's legitimate payment ecosystem and, thus, are laundered.

In a second method of transaction laundering, the same coffee mug company will set up their own stand-alone website on the clear web and will have coffee mugs for sale, along with product descriptions and prices. However, buyers in the know will understand the coffee mugs are a farce, as they are a front for illegal goods. Each type of coffee mug is representative of a different variety of drug, and the quantity of coffee mugs represents how many grams, or pounds, or kilos of drugs available. These coffee mugs can be paid for via credit card and are laundered through the legitimate payment ecosystem.

Theoretical Case Study – Continued

Going back to the theoretical example of Carlos the Cybercriminal, once he gains access to the compromised accounts via the credential stuffing campaign, he has the choice to cash out of the account or to sell the account reflective of the balance. If Carlos decides to cash out, he will first set up a new beneficiary account (usually a mule account), and then will transfer funds (usually via wire) from the compromised customer account into the mule account (Moneyval, 2012). Alternatively, Carlos could utilize a debit/credit card associated with the compromised account to withdrawal cash, which is then physically taken by a money mule, deposited into their account (or another mule/shell account), and then laundered overseas by one of the conduits described above.

If Carlos decided to sell the account for a price reflective of the balance (or some other variable), he would usually ask for digital currency, wire transfer, or money order as a form of payment. Using digital currency is most efficient as proceeds can instantaneously be transferred overseas into local fiat currency. If Carlos asks for payment in the form of another conduit (e.g., money order, wire transfer, etc.), the cybercriminal will designate a mule as the recipient of that wire/money order. The mule will then cash out and convert the money into another medium (e.g., wire, money order, digital currency, etc.) to transfer overseas (while keeping a small commission). Once the cybercriminal/organization ultimately receives the layered money, they will integrate the funds back into the economy by reinvesting in new tools and capabilities to better commit cybercrime or for many other reasons, such as directly supporting their operations or purchasing readily marketable goods (Moneyval, 2012). At this point, Carlos Cybercriminal will begin the cycle all over again. The two essential steps in this entire process are to turn the dirty money into cash and to utilize money mules (at some point in the process). This conversion makes

tracking the movement of money nearly impossible and solidifies the importance of money mules.

Real-Life Case Studies

Video Game Currency Investigation

Pivoting from the hypothetical to the practical/real world, this next section covers a few real-life case studies, which exemplify the convergence. In the 2018 FinCEN Director's Law Enforcement Awards Program, a cyber-based investigation was recognized for significant BSA reporting. The particulars of this case included a group of subjects who reverse engineered a video game (the cyber event) to fraudulently generate a large amount of in-game currency (the fraud). Once the in-game currency was generated, the subjects transferred that value off the account and converted it into fiat currency which would then be wired to various corporations offshore. From there, the money would be wired to individuals (money mules), who would then withdrawal it in cash and continue the laundering cycle. In the end, this scheme had generated over $17 million in proceeds which was used towards cash holdings and expensive assets. Once search warrants were issued and assets seized, over $10 million of fraudulent proceeds were forfeited, and four subjects pleaded guilty to numerous charges, including but not limited to money laundering, wire fraud, and conspiracy (Hudak, 2018).

Zeus Trojan Investigation

In 2010, the Manhattan U.S. Attorney charged 37 defendants in 21 separate cases that were involved in global bank fraud schemes which utilized malware to steal, and then launder millions of dollars. Specifically, the threat actors began to unleash cyberattacks (specifically the Zeus Trojan), targeting small businesses and municipalities in the United States. The Trojan sent a "benign" e-mail to these victims that installed a malware which recorded every keystroke once the link was clicked on. When the threat actors recorded the victim's bank logins, they would take control of the accounts and transfer thousands of dollars to different accounts set up by money mules. To recruit the money mules, the organization targeted individuals who entered the United States on student visas, provided them with fake foreign passports, and instructed them to open false-name accounts at U.S.-based banks. Once the bank accounts were opened, the wire transfers were deposited into these accounts, and the mules transferred the money overseas (after keeping a small commission), or they withdrew cash to be bulk smuggled out of the country. Over $3 million was stolen and laundered, all as the result of an "innocent" e-mail that generated malware (Manhattan, 2010).

Business E-Mail Compromise Investigation

In 2017, the U.S. District Attorney's Office for the District of Columbia unsealed four indictments that revealed multiple international fraud and money laundering rings. Business e-mail compromise was one of the main threat vectors utilized by the perpetrators who impersonated executive-level employees at mid-to-large size corporations. The threat actors (impersonating an executive) sent e-mails to mid-level employees instructing them to initiate

wire transfers from the company's corporate accounts to bank accounts controlled by the criminal syndicate. The mid-level employees were led to believe they were being entrusted to handle a large financial transaction as part of a secret corporate acquisition. Once the money was received by the criminal organization, it was quickly wired out of the accounts (e.g., layered) into China and ultimately delivered to the criminal organization in Eastern Europe. This scheme was conducted over a 13-month timeframe and generated over $10 million in proceeds (19 People, 2017).

FBI Operation Trident BreACH

In 2010, U.S., U.K., and Ukrainian authorities announced the arrest of over 100 individuals in one of the most successful international cyber investigations recorded, based on the number of arrests (Swecker, 2016). Five Ukrainian individuals were alleged to be the masterminds of this syndicate who created a Trojan that targeted small- to medium-sized businesses. This Trojan transmitted malware via a phishing e-mail wherein once the victim's financial accounts were accessed, the stolen funds were distributed to over 3,500 mules worldwide. The organizers recruited mules by providing them with counterfeit passports to open bank accounts. Once the mules received the stolen money, they would keep an 8–10% commission, and then transfer the money overseas. This cyber ring successfully stole and laundered at least $80 million dollars and attempted to steal over $220 million (Swecker, 2016).

Legislative and Regulatory Environment

The Budapest Convention

The current legislative and regulatory environment for financial institutions regarding cybercrime and the resultant reporting of such activities is murky, at best. In 2001, the Convention on Cybercrime was held in Budapest, Hungary, and was eventually ratified by 31 European countries and the United States (Moneyval, 2012). This treaty, referred to as the Budapest Convention, set up "the global framework of reference for cybercrime legislation" (Moneyval, 2012). Furthermore, the Budapest Convention generated a standard definition of cybercrime, required that members criminalize attacks against computer data and systems, put in place procedural measures for members to investigative cybercrime and resultant evidence apprehension, and set in place a foundation for members to cooperate and share intelligence (Moneyval, 2012). The Budapest Convention was the first international treaty to deal with such issues and was a good starting point, however, it lacked enough specificity to be tactically effective. Seventy-two percent of the world's countries have enacted cybercrime laws, which are all invariably different and inconsistent (Cabrera et al., 2018). Cyber events and cyber-enabled crimes are unique in that they occur instantly across international borders, but they also bring complexity for the same reason. For example, which country holds supervision authority in a cyber event? Is it the country in which the threat actors hold citizenship, or the country where the servers are located, or the country in which the victims live? These are still questions that are outstanding in the international arena.

Cybersecurity Information Sharing Act (CISA)

In terms of United States specific legislation, Congress passed the Cybersecurity Information Sharing Act (CISA) in 2015. CISA was designed to improve the cybersecurity landscape in the United States through the authorization of defensive measures and information sharing between the private sector and government. The legislation allowed for private companies to implement defensive measures to counter cyber threats, and provided certain protections for private companies to share cyber threat indicators and measures with the government (Karp & Weiss, 2016). However, information sharing is not mandatory, nor is there a standard for how or what data is shared. This same ambiguity applies to the AML realm, as information sharing is neither consistent nor clear between financial institutions and government.

OFAC's Cyber-Related Sanctions Program

In 2015, the Office of Foreign Assets Control (OFAC) implemented the Cyber-Related Sanctions Program and has issued resulting sanctions "against entities who are responsible for, are complicit in, or that have engaged in, certain malicious cyber-enabled activities, including by providing material and technological support to malicious cyber actors that have targeted U.S. organization" (Office, 2018). This is a unique challenge that financial institutions face as it varies from traditional list-based screening, whereas customers and transactions are compared against the OFAC list. In this circumstance, the software and technical services that a financial institution utilize must not have been derived from a sanctioned entity. Furthermore, banks need to ensure that their third-party service providers are compliant with these same regulations.

NYDFS Rule 500

In 2017, the New York Department of Financial Services (NYDFS) issued Rule 500, which implemented various cybersecurity requirements on all financial institutions regulated by this agency (which includes many operating in the United States). Rule 500 enacts several key requirements for financial institutions, such as establishing a formal cybersecurity program (including the designation of a chief information security officer), implementing and maintaining a formal written cybersecurity policy, having on-staff qualified cybersecurity personnel, and continual probing and testing of the institution's defenses. Rule 500 also requires that financial institutions notify NYDFS when a cybersecurity/cybercrime event occurs that has a reasonable likelihood of materially harming the normal operations of the institution within 72 hours (New York, Cybersecurity, 2017). Furthermore, financial institutions may have other state-specific regulations they need to comply with, depending on the location of their operations (such as NYDFS Rule 504, which requires senior leadership to certify to their programs AML effectiveness, among other items).

FinCEN Advisory on Cyber Events and Cyber-Enabled Crime

In 2016, FinCEN issued an advisory on cyber events and cyber-enabled crime. This advisory mandated Bank Secrecy Act (BSA) reporting on cyber events and cyber-enabled crime, but also emphasized that neither the advisory nor CISA changes existing BSA reporting requirements (i.e., SAR filings). The 2016 FinCEN advisory explicitly states that it is mandatory for financial institutions to file a SAR if it "knows, suspects, or has to reason to suspect that a cyber event was intended, in whole or part, to conduct, facilitate, or affect a transaction or series of transactions. Cyber events targeting financial institutions that could affect a transaction or series of transactions would be reportable as suspicious transactions because they are unauthorized, relevant to a possible violation of law or regulation, and regularly involve efforts to acquire funds through illegal activities" (Advisory, 2016). In determining if a cyber event meets the monetary threshold to file a SAR, a financial institution should consider "in aggregate the funds and assets involved in or put at risk by the cyber-event" (Advisory, 2016). From FinCEN's perspective, a simple intrusion into a bank's records by cybercriminals in which no money/data was stolen but was *potentially* compromised constitutes a SAR-reportable event. If accounts were monetarily compromised, or if personal information was compromised that could result in funds put at risk, a SAR filing is also warranted. FinCEN also encourages voluntary reporting of cyber events and cyber-enabled crimes when these events usually would not dictate the filing of a SAR, such as when hackers bring down a company's website.

ALTHOUGH FINCEN REQUIRES A SAR FILING FOR A CYBER EVENT OR CYBER-ENABLED CRIME, THE GUIDANCE IS NON-PRESCRIPTIVE.

As with many regulations, generally, FinCEN's guidance is interpretive and non-prescriptive. It leaves room for clarification on whether a cyber event constitutes a SAR filing for the financial institution. Consider the scenario of a threat actor successfully probing a financial institution's defenses and getting into the system without compromising customer's accounts or personally identifiable information. In that scenario, was it enough that assets were put at risk, and hence, a SAR filing is appropriate? Or does the financial institution need proof the threat actor tried to obtain account information and/or tried to conduct unauthorized transactions to consider the assets to be at risk? The FinCEN guidance leaves ambiguity in helping a financial institution draw a line in the sand between a reportable and non-reportable event. In the FAQs, FinCEN promotes voluntary reporting for unsuccessful attempts, however, a financial institution must take a risk-based approach and must consider the resources it takes (and takes away) in doing so. Financial institutions also must determine if filing a cumulative SAR to report multiple cyber events is appropriate, based on the similarities of each event via a risk-based approach (Advisory, 2016). It should be noted that the OCC, FDIC, and other regulators have issued additional guidance on the reporting of computer-related crimes for institutions that are covered by those entities.

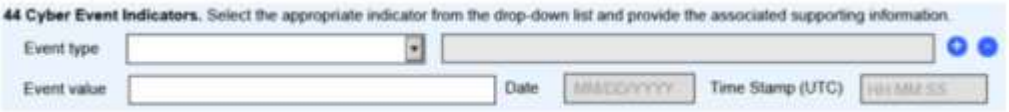
Regardless of the decision that financial institutions need to make on cyber-event SAR filings, all BSA reporting should encompass cyber-related indicators if available. In today's world, "financial transactions increasingly rely on electronic systems and resources, illicit financial activity often has a digital footprint which may correspond to illicit actors, their activity, and related suspicious transactions" (Advisory, 2016). It is highly recommended that any SAR should include all available cyber-related information available to the financial institution regardless of the typologies being filed on. These cyber indicators include but are not limited to: IP addresses with timestamps, e-mail addresses, URL/domains, virtual wallet information, device indicators, social media account/username information, etc. Obviously with SAR filings centered around specific cyber events or cyber-enabled crime, including more technical cyber indicators is appropriate (e.g., suspected malware filenames, browser details, command-and-control nodes, etc.). This information is vital to law enforcement as any small piece of financial intelligence such as an e-mail address can link previously unknown subjects together, identify more subjects and/or victims, and help trace the movement of illicit funds. On June 2018, FinCEN updated the SAR form with new fields and reporting options, many of which were related to cyber reporting. A new "Cyber event" suspicious activity type, a new text field to report IP and timestamp information, and new category fields to report up to 99 cyber events associated with suspicious activity were all added in this most recent update (below are sourced from FinCEN BSA, 2018).

Part II. Cyber event suspicious activity type (and associated subtypes)

- New "Cyber event" suspicious activity type category added to Part II.

Part II. New Cyber Event Indicators

- New category of fields to record up to 99 cyber events associated with the suspicious activity in Part II, including the event value (and date and timestamp, if applicable).



Part II. Date and Timestamp added to IP Address

- New text fields to accompany the IP Address field in Part II in order to record the date and/or timestamp of the first instance of the reported IP address.

As always, and with any SAR, a concise yet detailed description of the suspicious activity (including all pertinent cyber-related information) should be documented in the SAR narrative.

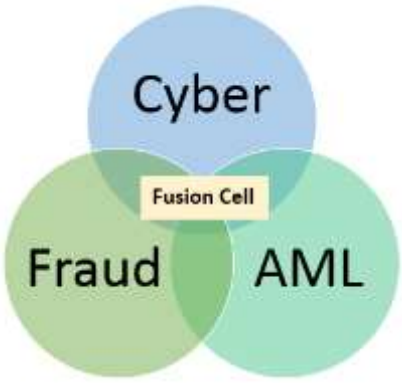
FinCEN requiring the reporting of cyber SARs is akin to the square peg (cybercrimes) going into the round hold (BSA). Even the 2015 Bitlicense legislation issued by the N.Y. Department of Financial Services states that virtual currency operators need anti-fraud, AML, and cyber units, but did not prescribe how to best combine the efforts of all three (New York, Bitlicense, 2015). In today's siloed environment, most AML financial intelligence units (FIU) do not have cyber expertise in-house. To file a quality SAR, the AML FIU needs information from the cyber unit and the fraud unit, and they need to fully comprehend the information to translate it into top-notch BSA reporting. Luckily, the FinCEN advisory does not mandate that AML professionals become experts in cyber, but how do financial institutions integrate these three silos?

Fusion Cell Approach

As complicated as the landscape of cybercrime can be, layer on top the complexity of implementing adherence to the regulations in an organizationally siloed environment. This perhaps creates the most pressing and technically complex issue with which the AML community has ever grappled. Specifically, the problem statement of how do financial institutions cohesively respond to the emerging cyber threat on an enterprise-wide basis while still maintaining full adherence to AML/BSA reporting will be addressed by the Fusion Cell approach. The Fusion Cell is a task force comprised of representatives across various departments that will address and maintain responsibility for the financial institution's enterprise-wide cyber policies and procedures. This model is not unlike some of the most powerful law enforcement collaborations (via task forces) that bring together multiple disciplines to fight a common enemy—think the El Dorado Task Force or the various HIDTAs (High Intensity Drug Trafficking Area task forces).

FINANCIAL CRIME RINGS RELY ON DATA AND PROCESS SILOES INHERENT WITHIN BANKS AND BETWEEN BANKS TO AVOID DETECTION (SWECKER, 2016).

The Fusion Cell should have oversight for the immediate response to any cyber event for the financial institution, from the initial IT technical investigation to the SAR filing/BSA fulfillment and notification of law enforcement. A Fusion Cell should be comprised of representatives from at least these areas: Cyber, Fraud, and AML. It is advisable to determine if other departments should be included, such as: Information Technology, Sanctions, Legal, and Advisory. In terms of who should be selected from each area, there should be a balance of both subject matter experts (SMEs) and mid-to-senior leadership able to make decisions and implement process changes within their organization. This permanent task force holds responsibility from the immediate event response to the holistic policy on cyber events as they are *the* convergence of Cyber, Fraud, and AML.



Guiding Principles

The World Economic Forum published four elements that public-private partnerships should follow in fighting cybercrime which financial institutions should adopt when forming the Fusion Cell: information sharing, cooperation, adherence and harmonization of existing laws, and issue discussion and resolution (Cabrera et al., 2018). Specifically, the goals of the Fusion Cell should be as follows:

I. Tactical Goals
   a. Coordinates the enterprise-wide response to material cyber events
   b. Delivers cyber-based AML/BSA reporting and contacts law enforcement (if applicable)
   c. Drives advanced analytics in identifying and responding to new risks (i.e., tuning)
   d. Meets on a regular cadence to identify new trends and communicates out to the larger audience

II. Holistic Goals
   a. Conducts an annual enterprise-wide cyber risk assessment
      i. Holds decision making ability to drive improvements from the assessment
   b. Develops enterprise-wide cyber response policy
   c. Provides regular updates to senior leadership/board of directors on the financial institution's response to events and resultant changes to policy
   d. Integrates internal referral process between Cyber, Fraud, and AML departments
   e. Provides oversight to ensure that the financial institution is complying with OFAC's Cyber-Related Sanctions Program
   f. Conducts overall training for Fraud and AML teams on cyber indicators

Talent and Resources

Once the members of the Fusion Cell are identified, they must be trained so that there is nothing lost in translation. At the onset, the biggest barrier to effective implementation of the Fusion Cell is if all parties are not speaking a mutually understandable language. Specifically,

when the cyber representative is relaying information, he or she must provide enough details and sufficient technical knowledge for all other parties to obtain a solid grasp of what is occurring. Similarly, the fraud and AML experts need enough cyber education to comprehend and 'translate' the information being relayed to them. This is the same as when the AML representative is speaking about typologies, movement of funds, and SAR/BSA requirements; all other parties need to have a grounded understanding to 'translate' that into deliverables from their area of expertise. If the cyber SME does not convey the technical information of a cyber event in an understandable context, how is the fraud SME supposed to identify the red flags and resulting financials for the AML SME to follow the money and convey the entire event into a chronological, clear, and concise SAR filing?

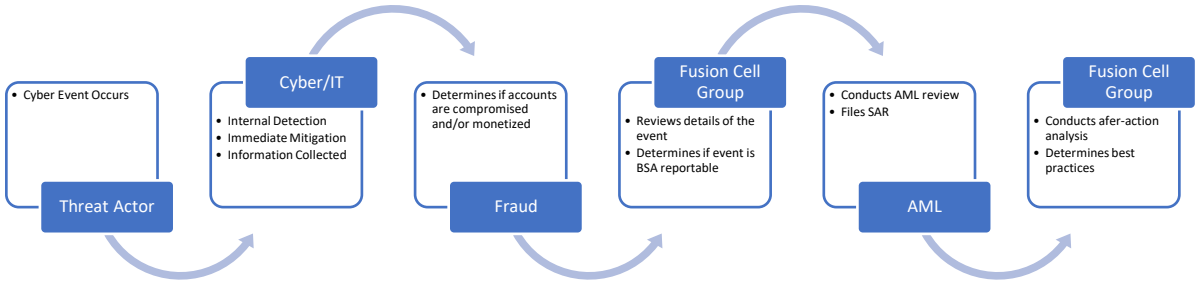
For this to happen, proper and formal training must occur for all parties. The recommendation of this white paper is that all non-cyber SMEs (i.e., representatives from Fraud and AML) go through formal cyber training, whether it is conducted by the financial institution or via external resources. Similarly, the cyber expert should go through Fraud and AML training for the same reasons. This training should not be as granular or extensive as if performing these functions daily. However, the training must be formal (it cannot be learn-as-you-go), must be detailed (so that every party has a working knowledge of other areas), and must occur before anyone new joins the Fusion Cell (so that there is seamless transition).

Governance and Operations

The next recommendation for the Fusion Cell is to meet on both an event-driven basis and a regular cadence. For an event-driven basis, the Fusion Cell should establish protocols on what type and magnitude of a cyber event constitutes assembly. This should be via a risk-based approach founded on the risk tolerance and resources of the financial institution. For example: Should the Fusion Cell convene when a simple intrusion was attempted but not successful? Or should it convene only when customer accounts were compromised, or could have been compromised? These are questions that the Fusion Cell needs to answer and will vary based on each individual financial institution. Furthermore, the Fusion Cell will need to create an internal referral process from any department in the institution to vet for potential adoption by the group. For example, if an AML investigator working on a case identifies concerning linkage between accounts that have enough cyber indicators to suggest a nexus, this would be referred over to the Fusion Cell for additional technical analysis and SAR filing.

The Fusion Cell is ultimately responsible to determine if a SAR filing is appropriate (based on the FinCEN guidance and the risk tolerance of the organization), at what point in the cyber timeline this should occur, calculating the monetary amount put at (or potentially put at risk), and ultimately filing the SAR and/or contacting law enforcement. Because experts from all the pertinent departments would be in the same room (Cyber, Fraud, AML), the Fusion Cell is in the best position to craft an accurate and comprehensive SAR filing for the institution—instead of AML just filing a SAR (in silo) with little context and pretext into the predicate activity. The below visual is meant to provide a high-level overview of the main responsibilities of each group during

an event-driven basis. Note that the tactical and logistical details will differ for each organization, and the Fusion Cell should have oversight and final decision-making approval for each step.



Next, the Fusion Cell not only needs to meet on an event-driven basis, but on a regular cadence to promulgate preeminence. Regular meetings would be utilized to analyze current trends, predict emerging trends, create after-action analysis, discuss efforts the financial institution is enacting that could change the operating environment, and provide training materials to employees in the broader departments. The Fusion Cell could also develop a data repository in which employees from Cyber, Fraud, or AML could query to improve their own independent investigations and to connect the dots in unforeseen ways. For example, an everyday AML investigator could query this database to provide IP address information in their normal SAR filings which would greatly benefit law enforcement. The Fusion Cell could institute oversight into creating advanced analytics and new rules that would specifically target suspicious activity related to the convergence of Cyber, Fraud, and AML to propel the financial institution into a proactive approach, and not just a reactive approach.

Further, the Fusion Cell should proactively benchmark to the industry and reach out to their regulators to determine best practices and key learnings. All parties, whether it is financial institutions or government entities, are in the same boat and are navigating these unchartered waters together. The financial institutions should also share as much nonproprietary information and financial intelligence as possible while collaborating.

The key to the Fusion Cell is that it follows a task-force/working group approach, but does not totally combine the AML, Fraud, and Cyber units. There is no practical way from a training, technology, system access, or cost basis to completely “break down the silos.” It is simply unreasonable to assume that breaking down walls between the three units is remotely possibly from an operational perspective; therefore, a working group approach is most prudent. Even if a financial institution could theoretically break down the silos, there is a legal risk that should be considered. According to some sources in the industry, “if Cyber and AML are merged and a bank is hacked and loses millions of dollars… (the bank) could potentially be prosecuted for failing to

put in place an effective AML program" (Wolf, 2016). Adopting the Fusion Cell methodology is the appropriate risk-based approach, brings alignment and shared knowledge to the various silos, confirms investigation findings, and ensures that a proper disposition was achieved for the company at large (Jones, 2014). Since the FinCEN guidance is non-prescriptive, it is up to the private industry to be proactive in identifying a solution to the proper convergence of Cyber, Fraud, and AML, and not wait to be told what to do.

Conclusion

"The convergence of money laundering and computer-based criminal activities is certainly not coincidental, particularly given the potential for large payoffs, the security of anonymity on the Internet, the relative ease of infiltration, and the natural barriers against capture and prosecution despite the risks" (Arrington, 2014). Besides drug trafficking, cybercrime is the most ubiquitous threat our financial system is challenged with today. Financial institutions face an even more complicated and nuanced challenge with cybercrime (both cyber events and cyber-enabled crimes) as a clear majority are not properly set up to handle these emerging threats. Many financial institutions are historically siloed, with Cyber, AML, and Fraud in separate departments under different reporting structures and leadership. A cyber event and/or cyber-enabled crime affects the company holistically and transcends the silos. How financial institutions conduct a risk-based approach to the convergence of these areas and how AML departments file informative and useful SARs is a daunting challenge.

Forming a Fusion Cell between Cyber, Fraud, and AML is the most prudent and risk-based approach that a financial institution can implement to combat the cyber challenge. It allows key subject matter experts and leadership to interact on an event-driven basis to counter and defend against the current threat, detect what assets are/were at risk, how funds were moved, and how to properly fulfill BSA requirements. A Fusion Cell should also meet regularly (not just event driven) to generate after-action reports, identify general and emerging trends, and develop training for the rest of the financial institution. Moreover, all staff within a financial institution should be given the basic foundational cyber training so that they recognize certain red flags and know when to escalate appropriately.

The cyber environment today is complex and ever-changing, and will only continue to become more ubiquitous across our everyday personal and professional lives. Cybercrime is the biggest but least understood threat that the AML community has ever faced. As an industry, it is easy to concentrate on the "shinier balls" like terrorist financing or human trafficking. While these typologies are critical to combat, detect, and deter, we cannot let the remediation of the cyber threat going by the wayside. The AML community cannot let the daunting challenge of tackling the cyber threat delay us, nor can we wait for regulators, or some other entity, to give us the blue prints to do so. "Operating in a silo within your own company and across the financial industry as a whole plays directly into the hands of malignant social networks" (Swecker, 2016). Right now, all financial institutions need to actively determine how to best build the interaction model

between Cyber, Fraud, and AML. It is impractical to combine these three units, but the proper convergence via the Fusion Cell approach will best combat the biggest threat our financial ecosystem faces today, the threat of cybercrime.

References

19 people indicted following investigations into international fraud and money laundering rings. (2017, March 1). U.S. Attorney's Office, District of Columbia. U.S. Department of Justice. Retrieved from https://www.justice.gov/usao-dc/pr/19-people-indicted-following-investigations-international-fraud-and-money-laundering

2016 Internet crime report. (2017). FBI & Internet Crime Complaint Center, 1–23. Retrieved from https://pdf.ic3.gov/2016_IC3Report.pdf

2018 Data breach investigations report. (2018). Verizon.

Abel, R. (2018, July 23). Cyber cartels launder money via gamer currencies. SC Media. Retrieved from http://www.scmagazine.com/home/security-news/cyber-cartels-launder-money-via-gamer-currencies/

Advisory to financial institutions on cyber-events and cyber-enabled crime. (2016, October 25). FinCEN, U.S. Department of Treasury, 1–9. Retrieved from https://www.fincen.gov/sites/default/files/advisory/2016-10-25/Cyber%20Threats%20Advisory%20-%20FINAL%20508_2.pdf

Alcantar, M. (2017, September 19). Cybersecurity: Nation-state actors, encrypted cybercrimes and man-in-the-middle attacks. *ACAMS Today*. Retrieved from https://www.acamstoday.org/nation-state-actors-encrypted-cybercrimes-man-in-the-middle-attacks/

Alexander, W. (2013, June 24). A chat with some immoral hackers who don't care about your feelings. Vice. Retrieved from https://www.vice.com/en_au/article/znqpj5/i-spoke-to-some-black-hat-hackers-about-internet-ethics

Arrington, B. (2014, August 28). What's cyber got to do with it? *ACAMS Today*. Retrieved from https://www.acamstoday.org/whats-cyber-got-to-do-with-it/

Bandler, J. (2017, June 9). Stemming the flow of cybercrime payments. *ACAMS Today*. Retrieved from https://www.acamstoday.org/stemming-the-flow-of-cybercrime-payments/

BSA e-filing system SAR updates & XML overview. (2018). FinCen, U.S. Department of Treasury, 1–38.

Business e-mail compromise: Cyber-enabled financial fraud on the rise globally. (2017, February 27). FBI News. Retrieved from https://www.fbi.gov/news/stories/business-e-mail-compromise-on-the-rise

Business e-mail compromise the 12 billion dollar scam. (2018, June 12). FBI, Department of Justice. Retrieved from https://www.ic3.gov/media/2018/180712.aspx

Copestake, J. (2014, September 19). Hiding currency in the Dark Wallet. BBC News. Retrieved from https://www.bbc.com/news/technology-29283124

dragonzz. (2018). Clearing up confusion – deep web vs. dark web vs. surface web. Steemit. https://steemit.com/blog/@dragonzz/clearing-up-confusion-deep-web-vs-dark-web-vs-surface-web

Cabrera E., McArdle, R., & U.S. Secret Service (CID). (2018, September 21). *The evolution of cybercrime and cyberdefense*. TrendMicro. Retrieved from https://documents.trendmicro.com/assets/white_papers/wp-evolution-of-cybercrime-and-cyberdefense.pdf

Criminals are using these tools to "crack" your website. (2017, Jun 12). SpyCloud. Retrieved from http://spycloud.com/tools-criminals-using-crack-website/

Cybercrime and money laundering. (2014). Eurasian Group on Combating Money Laundering and Financing of Terrorism. Retrieved from https://eurasiangroup.org/files/Typologii%20EAG/Tipologiya_kiber_EAG_2014_English.pdf

DEA Strategic Intelligence Section. (2017, October). *2017 national drug threat assessment*. Drug Enforcement Administration, U.S. Department of Justice, pp. 63–65. Retrieved from https://www.dea.gov/sites/default/files/2018-07/DIR-040-17_2017-NDTA.pdf

Frequently asked questions (FAQs) regarding the reporting of cyber-events, cyber-enabled crime, and cyber-related information through suspicious activity reports (SARs). (2016, October 25). FinCEN, U.S. Department of Treasury, 1–5. Retrieved from https://www.fincen.gov/sites/default/files/shared/FAQ_Cyber_Threats_508_FINAL.PDF

Gardiner, M. (2017, May 26). To guard against cybercrime, follow the money. *Harvard Business Review*. Retrieved from https://hbr.org/2017/05/to-guard-against-cybercrime-follow-the-money

Greenberg, A. (2014, April 29). 'Dark Wallet' is about to make bitcoin money laundering easier than ever. *Wired*. Retrieved from https://www.wired.com/2014/04/dark-wallet/

Heinzman, J. (2018, October 23).The ATM cash-out scheme and countering financial cybercrime. *ACAMS Today*. Retrieved from https://www.acamstoday.org/the-atm-cash-out-scheme-and-countering-financial-cybercrime/

Hudak, S. (2018, May 8). FinCEN director's law enforcement awards program recognizes significance of BSA reporting by financial institutions. FinCEN. Retrieved from https://www.fincen.gov/news/news-releases/fincen-directors-law-enforcement-awards-program-recognizes-significance-bsa

Jones, C. T. (2014, June 4). Cyber-response program: The first 48 hours…are you ready? *ACAMS Today*. Retrieved from https://www.acamstoday.org/cyber-response-program/

Karp, B. S. & Weiss, P. (2016, March 3). Federal guidance on the Cybersecurity Information Sharing Act of 2015. Harvard Law School Forum on Corporate Governance and Financial Regulation. Retrieved from https://corpgov.law.harvard.edu/2016/03/03/federal-guidance-on-the-cybersecurity-information-sharing-act-of-2015/

Kassner, M. (2015, February 2). Anatomy of the target data breach: Missed opportunities and lessons learned. ZDNet. Retrieved from https://www.zdnet.com/article/anatomy-of-the-target-data-breach-missed-opportunities-and-lessons-learned/

Khan, I. (2016, June). The virtual future of money laundering. *Fraud Magazine*. Retrieved from https://www.fraud-magazine.com/article.aspx?id=4294993747

Kruithof, K., Aldridge, J., Hetu, D. D., Sim, M., Dujso, E., & Hoorens, S. (2016). *Internet-facilitated drugs trade.* RAND Corporation. Retrieved from https://www.rand.org/pubs/research_reports/RR1607.html

Manhattan U.S. attorney charges 37 defendants involved in global bank fraud schemes that used 'Zeus Trojan' and other malware to steal millions of dollars from U.S. bank accounts. (2010, September 30). U.S. Attorney's Office, Southern District of New York. FBI. Retrieved from https://archives.fbi.gov/archives/newyork/press-releases/2010/nyfo093010.htm

McGuire, M. (2015, April). *Into the web of profit.* Bromium, Inc. Retrieved from https://www.bromium.com/wp-content/uploads/2018/05/Into-the-Web-of-Profit_Bromium.pdf

Meeuwisse, R. (2015–2017). *Cybersecurity for beginners*. London, UK: Cyber Simplicity Ltd.

Moneyval. (2012, March 9). *Criminal money flows on the Internet: Methods, trends, and multi-stakeholder counteraction*. Council of Europe. Retrieved from https://rm.coe.int/research-report-criminal-money-flows-on-the-internet-methods-trends-an/168071509a

Morgan, S. (2018, January 23). Top 5 cybersecurity facts, figures and statistics for 2018. News Online–Zeitschatten, CSO.

New York, Department of Financial Services. (2017, March 1). Cybersecurity requirements for financial services companies. Retrieved from https://www.dfs.ny.gov/legal/regulations/adoptions/dfsrf500txt.pdf

New York, Department of Financial Services. (2015, June 2). Bitlicense regulatory framework. Retrieved from https://www.dfs.ny.gov/legal/regulations/adoptions/dfsp200t.pdf

Office of foreign assets control cyber-related sanctions program risk management. (2018, November 5). FFIEC and OFAC. Retrieved from https://www.ffiec.gov/press/pdf/FFIEC%20Joint%20Statement%20-%20OFAC%20Cyber-Related%20Sanctions%20Program.pdf

Oyedele, A. (2017, May 6). BUFFETT: This is 'the number one problem with mankind'. Business Insider. Retrieved from https://www.businessinsider.com/warren-buffett-cybersecurity-berkshire-hathaway-meeting-2017-5

Paoli, G. P., J. Aldridge, N. Ryan, & R. Warnes. (2017). *Behind the curtain*. The RAND Corporation. Retrieved from https://www.rand.org/pubs/research_reports/RR2091.html

Survey: Majority of Americans reuse passwords and millennials are the biggest culprits. (2017, July 19). SecureAuth Corp. Retrieved from https://www.secureauth.com/company/newsroom/survey-majority-americans-reuse-passwords-and-millennials-are-biggest-culprits

Swecker, C. (2016, November). *The cyber crime wave: What bankers need to know*. Verafin. Retrieved from https://verafin.com/resource/cyber-crime-wave-bankers-need-know/

Teicher, R. (2017, August 23). Financial crime online: Dark web vs surface web. ITProPortal. Retrieved from https://www.itproportal.com/features/financial-crime-online-dark-web-vs-surface-web/

The ultimate guide to the dark web for law enforcement professionals. (2017). McAfee Institute. Retrieved from https://blog.mcafeeinstitute.com/the-ultimate-guide-to-the-deep-web-for-law-enforcement-professionals/

Townsend, K. (2017, January 17). Credential stuffing: A successful and growing attack methodology. SecurityWeek. Retrieved from https://www.securityweek.com/credential-stuffing-successful-and-growing-attack-methodology

Wolf, B. (2016, March 30). Link cyber and anti-money laundering units, but do not combine them—experts. Reuters. Retrieved from https://uk.reuters.com/article/idUS331585630120160330