E-COMMERCE

Illicit Actors' Use of Fraud and Reshipping Services

6 September 2019

2019
PUBLIC-PRIVATE
ANALYTIC EXCHANGE PROGRAM

2019 PUBLIC-PRIVATE ANALYTIC EXCHANGE PROGRAM

Table of Contents

Executive Summary

E-commerce: Illicit Actors Use of Reshipping Service addresses how illicit actors engage in fraud schemes to acquire funds used to support e-commerce fraud and reshipping schemes. E-commerce and reshipping fraud impacts four key sectors: retail, financial, shipping, and government. This six month study reviewed methods utilized by illicit actors to acquire funds, exploit retailers and financial institutions, obfuscate shipping processes, as well as the challenges with detecting this type of activity.

Addressing e-commerce and reshipping fraud will require collaboration between the retail, financial, shipping and government sectors to enhance current capabilities, develop new skillsets and increase information sharing. Each sector faces its own set of challenges to detect and disrupt this activity. It is likely this type of activity will only grow and becoming more challenging for the sectors to mitigate as illicit actors increase their use of emerging payment technologies to facilitate e-commerce fraud.

Scope

The E-commerce: Illicit Actors Use of Reshipping Services team ("E-Commerce Team") conducted a six month study examining how illicit actors engage in e-commerce fraud and utilize reshipping services as well as identifying the challenges encountered in detecting them. The E-Commerce Team conducted this study with the goal of identifying how illicit actors utilize emerging payment technology to engage in e-commerce fraud. Furthermore, the E-Commerce Team focused on how illicit actors purchase goods through e-commerce platforms and retail websites with illicit proceeds and how reshipping mules are utilized to reship goods domestically and internationally.

The E-Commerce Team conducted open source research as well as participated in conference calls and conducted an in-person research trip to Atlanta, Georgia to discuss the topic with individuals in the financial industry, fraud departments of major U.S. retailers, shipping companies, and members of the U.S. government, to include law enforcement agencies and a consumer advocacy organization. The information from the conference calls and research trip informed the team on how illicit actors are increasing their use of gift cards in engaging in e-commerce fraud and the types of goods illicit actors are seeking to purchase. Furthermore, the E-Commerce Team received information on the challenges with detecting and disrupting fraud schemes, such as information sharing between the public and private sectors, as well as reporting the activity to the appropriate entity.

Acknowledgements

The E-Commerce Team would like to thank the Department of Homeland Security and the Office of the Director of National Intelligence for supporting the 2019 Analytical Exchange Program. Furthermore, the E-Commerce Team would like to thank the individuals from the retail, financial, shipping, federal government and consumer advocacy groups that discussed this topic during conference calls and the research trip to Atlanta. Their insight and experience in these sectors was immensely valuable to the E-Commerce Team in conducting its research.

Team Members

The E-Commerce Team was compromised of the following members:

Tara H., *U.S. Customs and Border Protection (Team Champion)*

Divya B., *U.S. Department of Justice*

Nicholas Godin, The *MITRE Corporation*

Vasili M., *U.S. Customs & Border Protection*

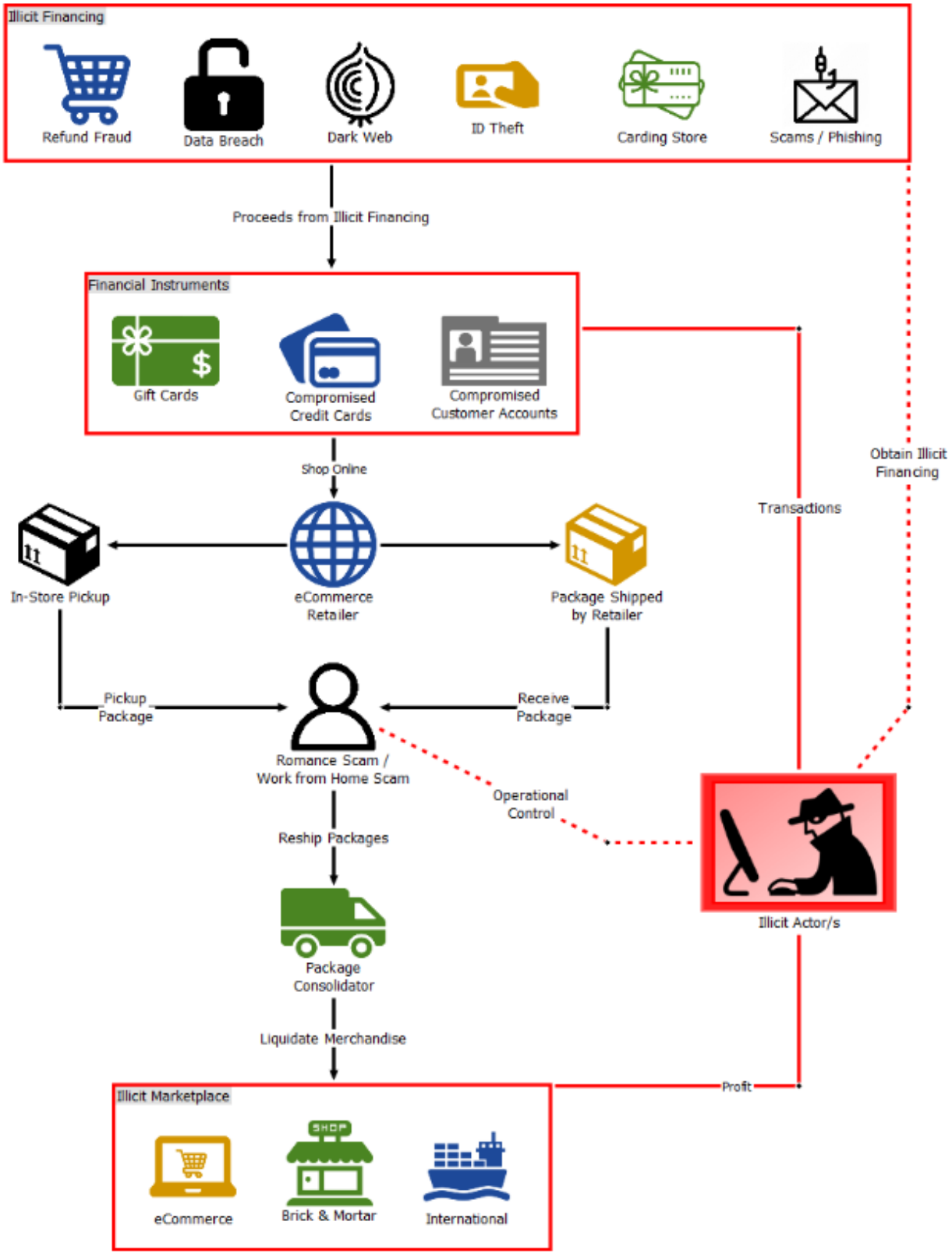
Jeremy M., *Federal Bureau of Investigation*

Charles Montgomery, *United Technologies Corporation*

Scott Peacock, *Walmart*

Molly Pro, *National Cyber-Forensics and Training Alliance*

E-Commerce and Reshipping Fraud Cycle



Illicit Financing: Financial Fraud and Money Laundering

Illicit actors rely on a number of financial fraud schemes to obtain and launder funds from victims within the U.S. Exploiting U.S. citizens and businesses is a profitable activity for illicit actors, and in 2018 generated approximately $3 billion in illicit proceeds from fraudulent financial activity. Illicit actors engage in a variety of illicit activities to obtain money that can be directly utilized or laundered to further conceal the source of money. Illicit actors engaged in e-commerce fraud have a number of options available to them to obtain money and drive their e-commerce activity.

- According to the 2018 Internet Crime Complaint Center ("IC3") yearly report, the IC3 received approximately 351,000 complaints with losses exceeding $2.7 billion dollars in 2018. These complaints are associated with crimes such as romance schemes, data breaches, identity theft, account takeovers, credit card fraud and re-shipping.[1]
- The Federal Trade Commission ("FTC") received approximately 1.4 million fraud reports in 2018, with losses of $1.4 billion, a 38% increase compared to 2017. One of the top schemes reported to FTC was identity theft, and credit card fraud on new accounts, with a 24% increase.[2]
- According to data from the Financial Crimes Enforcement Network ("FinCEN") regarding the filing of Suspicious Activity Reports ("SAR"), filings by depository institutions or money service businesses involving credit cards, debit cards or prepaid access rose from 186,723 in 2014 to 498,530 filings in 2018.[3]
- According to a 2019 examination of the Dark Web by Terbium Labs, 36% of the approximately 30,000 fraud guides analyzed mentioned payment cards. The guides identified credit cards as being more favorable to use for fraud compared to debit cards.[4]

Gift Cards

Illicit actors have increased their emphasis on acquiring gift cards as a method for defrauding victims, likely in part due to actions by the U.S. government to disrupt other forms of payments. As gift cards have gained popularity in society and are more frequently utilized to shop, gift cards provide illicit actors another way to purchase retail items while concealing the true nature of the source of funds. Criminal actors have turned to gift card schemes in particular to target the elderly and obtain funds that can be utilized immediately.

- According to Credence Research, a market research and consulting firm, the global gift card market was valued at $314 billion in 2017 and expected to reach $750 billion by 2026. Closed loop gift cards, which are cards that can only be redeemed at a single company, comprised 55% of the total market value with e-gift cards propelling overall market growth.[5]
- In 2018, the FTC noted that approximately 26% of all fraud victims reported being asked to activate gift cards or other forms of prepaid cards, a 270% increase from the 7% reported in 2015.[6]

- According to a 2018 Metro news article, the United States federal government has increased scrutiny on transactions involving financial instruments such as wire transfers and money. As a of result, the increased monitoring and the ripple effect following several high-profile court settlements, many consumer scams have shifted as fraudsters have made the transition to other financial instruments like gift cards in order to evade detection and continue their illicit operations.[7]
- According to a 2018 study by the FTC, adults in the U.S. age 60 and over reported paying money to a fraud scheme via prepaid card 17% of the time in 2017, resulting in a loss of $14 million dollars.[8]

An ancillary benefit of gift cards to illicit actors, is the ability to resell illicitly obtained gift cards for currency, further obfuscating the money trail that law enforcement may follow in trying to track illicit proceeds. The sale of illicitly acquired gift cards provides illicit actors the ability to utilize currency for other activity. Illicit actors can convert the proceeds from the sale of gift cards on a secondary gift card market place to another form of payment that could be utilized to fund e-commerce and/or reshipping fraud.

- According to cyber security expert, Brian Krebs, illicit actors prefer gift cards because they can easily convert the cards into a quick profit by selling them to one of the many online marketplaces like raise.com and cardpool.com. Krebs also notes that once an illicit transaction on the secondary gift card market has transpired, unwitting consumers later buy these cards at a steep discount and unbeknownst to them may inadvertently contribute to the perpetuation of unlawful activities.[9]
- In a 2018 study on gift cards and the secondary market, Loss Prevention Magazine, reported that the secondary gift card market offers an opportunity for illicit actors to convert fraudulently obtained gift cards into an estimated profit of 60-70% of the cards actual value. The study also found that in addition to using the secondary market, illicit actors can also convert their fraudulently obtained gift cards into cash through face-to-face transactions facilitated by platforms such as Craigslist where transaction fees can be avoided and profits of upwards 85-90% of a cards value can be obtained.[10]

E-Commerce: How Illicit Actors Commit Fraud and Adapt to Future Opportunities

Illicit actors are able to exploit different payment methods and shopping platforms and policies to obtain goods and move the goods around and out of the U.S. for a profit. As a result, innovations that should make life easier for the public, such as gift cards or online shopping, can assist illicit actors in obscuring their identity while engaged in illicit activity. The financial information illicit actors obtain from data breaches, credit card or identify fraud can be laundered and utilized for e-commerce and reshipping fraud.

- As of May 2017, a foreign illicit actor obtained personal identifiable information ("PII") through the compromise of a computer database and utilized the information to file false federal tax returns and received the tax refunds on gift cards. The gift cards were utilized to purchase electronic merchandise which was then shipped to South America utilizing U.S.-based reshipping services according to a U.S. Department of Justice ("DOJ") press release.[11]
- According to a 2017 DOJ press release, an illicit actor posed as an employee of multiple businesses and engaged in the unauthorized purchases of merchandise, which was then directed to U.S.-based individuals acting as re-shippers who would ship the merchandise overseas or would sell the products online.[12]
- According to a 2018 DOJ press release, three illicit actors stole and sold over 2,700 consumer electronic items by exploiting a major retailer's fraud department. These individuals made false allegations that the electronic goods, such as digital cameras and smartwatches, they ordered and received were damaged or non-working, subsequently requesting replacements at no cost. This fraud scheme totaled over $1.2 million in an attempt to fraudulently obtain electronic goods. Once this aspect of the scheme was complete, another illicit actor then purchased the above-mentioned electronic items and re-sold them, then ultimately re-sold to the public through an e-commerce platform. In the course of this activity, the illicit actors operated a multi-person fraud scheme in order to defraud a major retailer in an attempt to reap the rewards of reshipping fraud.[13]

Exploitation of Shopping & Payment Technology

Technology has changed both the way the public shops and pays for goods and services, presenting opportunities for the financial and retail sectors to reach a larger segment of the public and increase sales. However, illicit actors are able to exploit the same conveniences in shopping and payment technology to commit e-commerce fraud and acquire goods to be passed on to shipping mules.

Retail Technology

The retail industry has seen a growing increase in commerce shifting from brick and mortar stores to online activity. As the retail industry continues to shift more activity online through computers, tablets and smartphones, and implemented easier ways to place and retrieve orders, illicit actors will have increased opportunities to victimize both individuals and retail companies. Illicit actors will have more avenues to engaging in e-commerce fraud through different types of devices and applications, providing additional opportunities to conceal their illicit activity.

- A 2018 Experian research study found most consumers own a smartphone (91%) or a laptop (83%) and have embraced their mobile devices to conduct digital commerce with online shopping (90%) and personal banking (88%) being the most common activities.[14]
- In a 2018 mobile payments study, Kount, a fraud prevention and digital innovation firm, reported that trends in the mobile payment industry indicated that more users were likely

to come online with nearly one-third of merchants expecting mobile payments to account for at least 50% of their total revenue by year 2020 with more merchants planning to bring mobile applications for online shopping purchases rather than relying on a dedicated mobile website.[15]

- Riskified, a fraud prevention and innovations company, noted in a 2019 e-commerce fraud trends report that automation will play a bigger role in the ordering process as retailers move toward fully automated fulfillment and shipping centers. The move toward automation will benefit retailers in terms of reduced costs and will enable customers to receive their products more efficiently; however, increased automation also introduces new fraud threats. For example, customers often only need a pickup authorization number or token to receive their merchandise at a delivery kiosk. E-commerce retailers will require heightened awareness of these types of transactions to ensure that the package receiving process is not being abused.[16]

Payment Technology

The development of new payment technologies by both the financial and retail sectors has provided the public more ways to pay for goods and services. As retailers increase the methods by which they will accept payment and as these methods become more widely used by the public, illicit actors will diversify the way goods are paid for on e-commerce platforms. While payment methods like gift cards provide illicit actors a method to pay for goods that can obfuscate their true identity, other technology such as mobile wallets and cryptocurrency are likely to attract illicit actors as it will allow them to diversify their methods of engaging in illicit e-commerce transactions.

- A 2018 mobile wallet usage report found mobile wallet technology will continue to grow around the world. China has been an early adopter of the technology with 47% of the country actively transacting on mobile payment platforms such as Alipay and WeChatPay. In contrast, the United States has been relatively slow to adopt mobile wallets with only about 17% of the country using mobile wallet technology.[17]
- According to a 2019 study by Riskified, more customers demanded the ability to shop and pay via apps such as Venmo and Zelle. An estimated 40% of smartphones will have these types of apps installed in 2019 and retailers will be working to accept these forms of payment. U.S. millennials are 41% more likely to shop via mobile apps than baby boomers, and they expect a seamless mobile payment experience.[18]
- CNBC in a 2018 news report noted cryptocurrencies represent another potential vector that fraudsters could attempt to exploit. Though in its infancy as an industry and not widely available, companies are shifting and making it easier for customers to conduct transaction with cryptocurrency.[19] For example, Flexa, via its Spend app, allows customers to process payment transactions with Bitcoin, Ether, Bitcoin Cash, and the Gemini dollar at any merchant currently accepting payments on the Flexa network. This represents a significant breakthrough as customers can now transact at stores in real time without the uncertainty and volatility often associated with the crypto market. Flexa can offer these advantages by

not tying cryptocurrency payments to debit cards but rather establishing new connections with point-of-sale terminals and completely bypasses existing infrastructure.[20]

- Juniper Research, a digital trends and research consultancy group found that with the advent of Europay, Mastercard, & Visa credit card transactions in 2015, retailers in the United States have seen a shift from traditional fraud in brick and mortar stores to card not present and mobile wallet fraud via e-commerce platforms. Additionally, new payment systems such as application of programming interface driven 'banking-as-a-service' applications offer new avenues for illicit actors to exploit. Due to these shifts, estimates suggest that annual losses associated with e-commerce fraud topped $22B in 2018 and will continue to rise to upwards of $48B by 2023.[21]

Shipping: Moving Goods & Recruiting Mules

Obscuring one's identity as an illicit actor is most important at the shipping stage of an e-commerce scheme. In order for illicit actors to monetize their purchases, they will need to move fraudulently obtained goods within the U.S. for possible resale or export them from the U.S. for disposition. Therefore, illicit actors have to recruit mules, or obtain the services of mules, as the labor to support reshipping schemes. Use of a mule will anonymize the shipping and further mask the identity of the illicit actor.

- According to a 2018 article by Experian, online shopping fraud rose 30% in 2017 compared to 2016. Experian found rates of billing fraud, which occurs when a victims address is tied to the payment account, rose by 34% in 2017 compared to 2016 while rates of shipping fraud, which occurs when a criminal used their address for the delivery of stolen goods, rose by 37% in 2017.[22]

Shipping Scam Process

After a fraudulent e-commerce procurement, the good(s) are, more than likely, shipped to a mule with a U.S. mailing address. By using a mule's U.S. address, or a third party's U.S. address, the illicit actor may circumvent preventative measures implemented by most e-commerce vendors to avoid unrecoverable international shipments. After a fraudulent e-commerce transaction passes an e-commerce vendor's internal fraud filters, the purchased goods are unknowingly shipped to the address of the mule.

- According to U.S.-based logistics company UPS, a fraud scheme such as the "returns processing position" is utilized by illicit actors who hire employees to receive and process incoming packages from a fictitious company's clients. These fraudulent companies sell goods such as electronics, and the employee inspects the package and follows instructions by the "Returns Manager" to repack and reship the merchandise.[23]
- As of April 2016 RSA, a U.S.-based cybersecurity company, indicated operators of fraud chain's usually discontinue the use of reshipping mules after no more than 30 days, and before the mule would expect to receive their first check for the work they performed. Mules can be obtained from fraud-as-a-service providers operating on the darkweb.[24]

Illicit actors utilize a variety of methods to identify and recruit individuals to participate in reshipping schemes. Recruiting through seemingly legitimate job opportunities as well as utilizing dating websites provides illicit actors multiple avenues to identify and recruit mules. As a result, illicit actors are likely to recruit individuals who are unaware of the true nature of their work either through belief that they have gained a new job opportunity or due to personal feelings. After recruitment, many of these mules do not realize they are subject of a recruitment scam or participating in fraudulent activities until they either fail to receive payment for their time and other expenses or are contacted by law enforcement authorities. To keep the scam fresh and dynamic, illicit actors will often employ similar recruiting and pre-employment techniques as popular companies to legitimize the appearance of their operation.

- According to the 2018 Better Business Bureau ("BBB") Scam Tracker Risk Report, "Scammers conduct in-depth interviews via Google Hangouts and other technologies, provide employment forms, and ask scam targets to perform job duties before the scam is discovered."[25]
- According to Agari, a U.S.-based email security company, commonalities associated with recruiting shipping mules include use of the job title "Reshipping Agent", broken English and grammatical errors are present throughout the listing, the company is never identified, only correspondence is via email and a telephone number or address is not present in the posting.[26]
- As of May 2016, the U.S. Attorney's Office for the Southern District of Mississippi identified multiple Nigerian individuals who engaged in a scheme dating back to 2001 to identify and solicit individuals through dating websites and work-at-home opportunities to receive and ship merchandise purchased with stolen PII, such as cell phones.[27, 28]

Combating E-Commerce & Reshipping Fraud: Government Limitations

Government efforts to combat e-commerce fraud and reshipping schemes involve both investigative and regulatory action at the federal and state level. Efforts to coordinate the reporting of fraud as well as combatting the illicit movement of money and goods involves both government agencies involved in conducting investigations as well as investigations implementing and enforcing regulations.

Investigation vs. Regulation

Government efforts to combat e-commerce and reshipping fraud relies on action involving both the investigation of illicit actors and the regulation of industry to prevent illicit actors from engaging in these types of crimes. This balance of investigation and regulation is largely an issue for the federal government, but state regulatory agencies as well as state and local law enforcement agencies play a role in preventing, detecting and disrupting this activity.

Reporting Fraud

Identifying fraud associated with e-commerce and reshipping scams is a challenge due to the diverse number of criminal activities involved. Identity theft, credit card fraud, wire fraud, mail fraud and money laundering are just some of the criminal activities illicit actors are involved in. These types of crimes may be worked by multiple federal, state and local law enforcement agencies presenting opportunities for both cooperation and jurisdictional challenges for law enforcement agencies. Furthermore, it also becomes an issue of government regulation, with other agencies examining the issue from a regulatory view. As a result, the U.S. government has multiple venues for victims to report instances of fraud.

- The U.S. government operates multiple websites managed by different U.S. government agencies, such as the U.S. Postal Service ("USPS"), the Consumer Financial Protection Bureau to report various types of fraud such as mail fraud or credit fraud. The U.S. government also collaborates with foreign governments to operate econsumer.gov, which is a collaboration of consumer protection agencies from 33 countries.[29, 30]
- The Federal Bureau of Investigation's ("FBI") IC3 and the FTC's Consumer Sentinel database both operate databases that can be utilized by law enforcement to identify victims or subjects associated with fraud schemes. FTC's database also includes information from the USPS – Office of Inspector General, as well as U.S. BBB and international data from Canada.[31, 32]

Cargo Inspections

E-commerce has significantly altered the international trade environment, challenging U.S. Customs and Border Protection ("CBP") to modify its approach to legitimate trade facilitation, trade compliance regulation enforcement and cargo security. Even though many security and information collection programs have been implemented since 9/11[1] by the U.S. Government that can potentially be a deterrent to illicit e-commerce activity, these programs require an expanded scope to become omnidirectional (*i.e.*, imports and exports). Only then will they be successful at detecting illicit e-commerce shipping activity. CBP and transportation service providers need data to analyze reshipping patterns and trends resulting from illicit e-commerce schemes.

- According to testimony before the U.S. Senate in 2018, the Commissioner of CBP indicated the passing of the Trade Facilitation and Trade Enforcement Act of 2015, Congress increased the de minimis value from $200 to $800. Industry impact resulting from this change has caused a dramatic shipping volume increase of low value e-commerce shipments imported into the U.S. significantly altering the dynamics of the international trade environment and CBP's ability to enforce trade laws.[33]
- According to testimony before the U.S. Senate in 2018, the Commissioner of CBP indicated that CBP is now collecting advance electronic data on some imported de minimis shipments (*i.e.*, shipments valued at $800 or less). In addition, a new special entry type

[1] See Appendix A: Department of Homeland Security Cargo Screening Programs for additional information on DHS cargo screening programs established post-9/11

(*i.e.*, type 86) is being implemented for e-commerce de minimis shipments to facilitate identification and movement of these low value shipments. As with the other previously discussed post 9/11 (*i.e.*, September 11, 2001) regulatory and enforcement changes, this e-commerce de minimis shipment data collection involves data collection, advance shipping information analysis of advance shipping information and screening of imported goods prior to their arrival into the U.S.[34]

- According to testimony before the U.S. Senate in 2018, the Commissioner of CBP stated "Over the past five years, CBP has seen a nearly 50 percent increase in express consignment shipments, and an astonishing 200 percent increase in international mail shipments."[35]

Illicit Financial Activity

Detecting and disrupting illicit financial activity is a responsibility of both regulatory and law enforcement agencies within the U.S. While an agency like FinCEN regulates how the financial industry files SARs documenting suspicious financial transactions, law enforcement at all levels investigates financial fraud and money laundering. There is also the overlap in which some law enforcement agencies are able to access and review FinCEN SARs to support investigative efforts. This collaboration is beneficial for the government sector to identify illicit financial activity. However, challenges still remain to adapt to emerging payment technologies.

- As of 2018, FinCEN's SAR electronic filing requirements guide does not include cryptocurrencies or mobile wallets in their list of payment mechanisms. The only places to document these payment methods is in a field labeled as "other."[36]
- Between January 2017 and June 2018, approximately 25% of FBI main case subjects were linked to FinCEN reporting, an increase of approximately 9% in 2012.[37] As of 2018, approximately 24% of U.S. Internal Revenue Service's ("IRS") investigations are based on FinCEN information.[38]
- As of 2018, FinCEN had provided support to over 100 cases since 2016, providing support to "law enforcement, regulators, and prosecutors" to identify, trace, and analyze virtual currency activity. Analysis conducted by FinCEN estimates since 2011, $4 billion in virtual currency has moved through the darkweb.[39]

Law Enforcement Coordination

The coordination and deconfliction of criminal activity between approximately 18,000 federal, state, and local law enforcement agencies is a challenging effort despite efforts at all levels of law enforcement to collaborate. While the use of task forces, working groups, and intelligence sharing can lead to successful efforts in connecting illicit actors across jurisdictional lines, criminal groups are likely benefitting from a large and diverse law enforcement system within the United States.

The overlap and separation in missions and jurisdictions presents an opportunity for illicit actors to engage in e-commerce fraud and reshipping scam activity that may be beyond the scope

of some law enforcement agencies, while other agencies may not pursue individual actors due to the lack of prosecutorial interest or shortage of investigative resources.

Furthermore, how individual agencies investigate these frauds can widely vary, for some agencies the issue may be considered cybercrime, organized crime, money laundering, or identity fraud. At the federal level, agencies may miss opportunities for investigating this type of activity as agencies may classify criminal activity as one type of crime and not collaborate within their own agency or with other federal agencies. At the local law enforcement level, what may be considered a case of credit card theft could be part of a larger money laundering conspiracy investigated by a federal law enforcement agency.

- The investigation lead by the USAO-SDMS highlighted above, involved the collaboration of the USPS-OIG, the USSS, HSI along with cooperation from the Toronto Police and multiple South Africa law enforcement prosecutorial agencies. Other investigations highlighted in this paper have involved the FBI, IRS, U.S. Marshalls Service and a state police department.[40,41, 42, 43]
- Between 2017 and 2018 multiple federal and state agencies investigated e-commerce fraud resulting in a number of different charges such as mail fraud, wire fraud, unauthorized access, aggravated identity theft, and money laundering.[44, 45, 46, 47]
- The FBI's Operation Wellspring Initiative combats internet based fraud schemes by referring criminal complaints not meeting most federal investigative thresholds to state and local officers embedded on Cyber Task Forces ("CTF"). As of 2018 the FBI operated CTFs in 13 of its 56 field offices and referred 123 complaints to CTFs based on complaints, associated with approximately $28.1 million in victim losses.[48]

Technology Challenges to Law Enforcement

Investigations into crime associated with e-commerce fraud and reshipping schemes likely requires law enforcement agencies to obtain data, such as financial and communication information, from financial institutions, telecommunications providers and retail companies. Additionally, search warrants executed by law enforcement may result in acquisition of electronic devices such as cellphones, computers and tablet devices. Investigations into e-commerce and reshipping schemes can slow down once law enforcement collects electronic data from subpoenas and search warrants. A contributing factor to this slowdown is the level of training and staffing law enforcement agencies have to analyze and exploit electronic evidence.

Data Acquisition

Furthermore, the adoption of new methods and platforms – blockchain technology-based or encrypted mobile apps, to name a few – comes with two major challenges: they are highly sophisticated and technical, which makes it harder to hire qualified personnel; and high encryption capabilities makes it very challenging, in some cases impossible to identify the entities behind illicit activity.

- According to a 2018 Rand Corporation study, obtaining content records, such as the text of an email, from electronic communication services that has held records for 180 days or less requires a warrant for access, however, records held for greater than 180 days can be obtained with a court order. Non-content records, such as internet protocol (IP) addresses may be obtained with a subpoena without notice.[49]
- According to a 2018 study conducted by the Center for Strategic and International Studies ("CSIS"), law enforcement requested approximately 600,000 requests for digital evidence such as communications content and metadata to nine U.S.-based technology and communications companies, AT&T, Verizon, Comcast, Google, Facebook, Microsoft, Twitter, Apple, and Oath during 2017.[50]
- According to a 2018 study conducted by the CSIS, extracting data from mobile devices may require the use of equipment that costs thousands of dollars or require law enforcement to utilize tools to parse data sets returned by service providers or to decrypt data that was sent in an encrypted form.[51]

Data Exploitation

Law enforcement has continually sought to enhance their ability to analyze digital evidence as illicit actors have exploited technology for illicit activity. While many law enforcement agencies, regardless of jurisdiction, have their own personnel to exploit digital evidence, many agencies do not have that capability or may face competing priorities to analyze data for other investigations. While the Department of Justice operates Regional Computer Forensics Labs ("RCFL") which can provide assistance to local law enforcement, however, several regions throughout the country do not have access to a RCFL.

Additionally, as the idea of "Big Data" has gained popularity, incorporating data analytics into how law enforcement exploits data is an emerging challenge. Recruiting and adding positions such as data analysts and data scientists is likely an area law enforcement agencies are attempting to address in order to fully exploit data obtained from investigations.

- As of August 2019, the FBI operates 17 RCFLs in 14 states. These RCFLs provide digital forensics training and support to federal, state, and local law enforcement agencies. RCFLs provide direct support on a case-by-case basis and are staffed by approximately 10-12 examiners.[52]
- According to a survey conducted by the CSIS in 2018, only 58% of respondents "felt their department has access to the resources...needed to meet their digital evidence needs". Of those surveyed, 95% had requested digital evidence assistance from the past year from a state or local laboratory or federal agency.[53]

E-Commerce Fraud & Reshipping Fraud: Emerging Issues

E-commerce and reshipping fraud are likely to remain a challenge to the retail, financial, shipping and government sectors for two distinct reasons: the increase in emerging payment methods and the challenge of "Big Data".

As the retail, financial and shipping industries continue to offer new platforms to purchase goods and services, illicit actors will likely exploit these offerings for their own activities. The expansion of payment technologies such as mobile wallets and cryptocurrency will continue to offer illicit actors new and diverse ways to conceal the true source of illicitly obtained funds and make it challenging for retail and financial sectors as well as the government to identify fraudulent transactions and who is behind those transactions.

The increase in e-commerce activity and the financial data associated with those transactions creates a "Big Data" problem for the financial, retail, shipping, and government sectors. The fraud departments of the private sector entities will have increased data they analyze to identify fraudulent activity impacting their business operations. The government sector's challenge will be how to identify, obtain, and analyze the data the private sector collects on fraudulent financial transactions and e-commerce orders. During the course of law enforcement investigations, data obtained from court orders can provide law enforcement access to financial and communication data that is utilized to build out the illicit networks involved in e-commerce and reshipping fraud. As more and more commerce shifts online it increases the amount of data that law enforcement can collect, however, having the training and resources to analyze the data will be a challenge for law enforcement at all levels of government.

E-Commerce & Reshipping Fraud: Challenges & Recommendations

Private and public sectors face challenges in detecting and disrupting e-commerce and reshipping fraud. The major challenge impacting both sectors is how to identify this activity, whether it's a retailer trying to determine if a transaction is fraudulent or for a law enforcement agency to identify if, and how, one instance of fraud may be related to a larger network of illicit actors.

As such there are three main challenges the private and public sectors face in identifying and disrupting this fraud and the E-Commerce Team identified several recommendations to mitigate these challenges.

Challenge: Overlapping mechanisms for victims to report fraud exist in the public and private sectors; the U.S. government has multiple databases to check for reporting on fraudulent activity.

- **Recommendation:** Ensure federally-operated fraud reporting databases facilitate information sharing between databases operated by different agencies and to increase usage by law enforcement personnel at all levels.

- **Recommendation:** Coordinated between public and private sector entities to encourage the public to report instances of fraud to the appropriate government agencies when contacting retailers to report fraud.

Challenge: Detecting new methods and shifts in tactics utilized by illicit actors to acquire and launder money used to facilitate e-commerce and reshipping fraud.

- **Recommendation:** Improve the ability of financial institutions and retailers to report illicit financial transactions involving emerging payment methods by updating fraud reporting sites and FinCEN SAR forms to include categories for new payment methods such as mobile wallets and cryptocurrencies.
- **Recommendation:** Enhance gift card security and fraud awareness through collaboration among the retail, financial and government sectors.

Challenge: Collecting & analyzing digital evidence and "Big Data" sets to identify illicit activity.

- **Recommendation:** Increase training and staffing for digital evidence and data analytics positions within the federal, state and local law enforcement agencies.
- **Recommendation:** Strengthen mechanisms at the federal level to encourage the use of data analytics by law enforcement agencies and collaborate with the private sector to develop best practices for identifying e-commerce fraud.

Implementation of these recommendations can benefit both the private and public sectors. U.S. Government efforts can alleviate an underlying concern of a lack of information sharing between the public and private sector. Improvements by the public sector to streamline and better coordinate efforts to report fraud, analyze digital evidence and identify illicit financial transactions can provide the government more accurate information regarding trends in e-commerce and reshipping fraud that can be passed on to the private sector.

Appendix A:
Department of Homeland Security Cargo Screening Programs

In 2004, the 9/11 Commission's final report identified the security of international transportation networks as a risk. In order to secure these transportation networks destined to the U.S., numerous organizations and programs were established to screen and collect shipment information on arriving cargo. Organizations created under DHS to accomplish this task included the:

- *Transportation Security Administration ("TSA"):* Established to protect the nation's transportation systems to ensure freedom of movement for people and commerce.[2]
- *U.S. Customs and Border Protection ("CBP"):* Formed in March 2003[3] under DHS as one of the largest and most complex components of DHS. CBP also has a responsibility for securing and facilitating trade while enforcing hundreds of U.S. regulations.[4]
    - *Centers of Excellence and Expertise ("CEE"):* Established to align with modern business practices to focus on industry-specific issues. The national authority afforded CEEs broadens CBP's capacity to identify systemic trade violations and strengthening detection and intervention techniques to fine-tune detection of illegitimate business.[5]
    - *National Targeting Center*: Established to coordinate and support CBP anti-terrorism activities relating to cargo movements by proactively targeting high-risk shipments.[6]

Procedural changes and programs implemented by these agencies include the:

- *Certified Cargo Screening Program ("CCSP")* to achieve 100% screening of cargo transported on passenger aircraft.[7]
- *Customs Trade Partnership Against Terrorism ("CTPAT")* is a voluntary public-private sector partnership program to strengthen the security of the international supply chain.[8]
- *Container Security Initiative ("CSI")* identifies for inspection and inspects ocean containers in foreign ports before they are placed on vessels destined for the United States.[9]
- *Import Security Filing ("ISF" or "10+2")* requires importers and carriers to submit Mandatory Advanced Electronic Information for ocean cargo destined to the U.S.[10]
- *Automated Targeting System ("ATS")* is a decision support tool that compares traveler, cargo, and conveyance information against law enforcement, intelligence, and other enforcement data using risk-based scenarios and assessments.[11]
- *Air Cargo Advanced Screening ("ACAS")* requires submission of advanced air cargo information on shipments arriving by air into the U.S. from foreign locations.[12]

---

2 https://www.tsa.gov/about/tsa-mission
3 https://www.cbp.gov/about/history
4 https://www.dhs.gov/operational-and-support-components
5 Kevin McAleenan, Testimony to U.S. Senate Committee on Finance, (July 18, 2018)
6 https://www.cbp.gov/frontline/cbp-national-targeting-center
7 49 C.F.R. § 1549, Certified Cargo Screening Program
8 https://www.cbp.gov/border-security/ports-entry/cargo-security/ctpat
9 6 U.S.C. § 945, Container Security Initiative
10 https://help.cbp.gov/app/answers/detail/a_id/1707/~/import-security-filing-%28isf%29---when-to-submit-to-cbp
11 https://www.dhs.gov/publication/automated-targeting-system-ats-update
12 Federal Register, Vol. 83, No. 113, p. 27380 (June 12, 2018)

Endnotes

[1] IC3. (2018). 2018 Internet Crime Report. Retrieved from https://www.ic3.gov/media/annualreport/2018_IC3Report.pdf

[2] FTC. (2019, March 1). The Top Frauds of 2018. Retrieved from https://www.consumer.ftc.gov/blog/2019/02/top-frauds-2018

[3] FinCEN. (2019). SAR Stats. Retrieved from https://www.fincen.gov/reports/sar-stats

[4] Whitney, L. (2019, April 17). How criminals use fraud guides from the Dark Web to scam organizations and individuals. Retrieved from https://www.techrepublic.com/article/how-criminals-use-fraud-guides-from-the-dark-web-to-scam-organizations-and-individuals/

[5] Credence Research. (2018). Gift cards market, size, share, trends and forecast to 2026. Retrieved from https://www.credenceresearch.com/report/gift-cards-market

[6] Fletcher, E. (2018). Scammers increasingly demand payment by gift card. Retrieved from United States Federal Trade Commission website: https://www.ftc.gov/news-events/blogs/data-spotlight/2018/10/scammers-increasingly-demand-payment-gift-card

[7] Morris, M. (2018). Why online scammers ask for an iTunes gift card. *Metro*. Retrieved from https://www.metro.us/news/the-big-stories/itunes-gift-card-scam

[8] FTC. (2018, October 18). Protecting Older Consumers. Retrieved from https://www.ftc.gov/system/files/documents/reports/protecting-older-consumers-2017-2018-report-congress-federal-trade-commission/protecting_older_consumers_-_ftc_report_10-18-18.pdf

[9] Krebs, B. (2015). The role of phony returns in gift card fraud. Retrieved from https://krebsonsecurity.com/2015/12/the-role-of-phony-returns-in-gift-card-fraud/

[10] Atamer, A., & Eng, S. (2016). Craigslist and the potential for gift card fraud. Retrieved from https://losspreventionmedia.com/craigslist-and-the-potential-for-gift-card-fraud/

[11] DOJ. (2017, April 17). Man Admits Guilt in Stolen Identity Refund Fraud Scheme Using Hacked UPMC Employee Information. Retrieved from https://www.justice.gov/usao-wdpa/pr/man-admits-guilt-stolen-identity-refund-fraud-scheme-using-hacked-upmc-employee

[12] DOJ. (2017, June 27). McKeesport Man Pleads Guilty in FBI Investigation into Fraud Scheme. Retrieved from https://www.justice.gov/usao-wdpa/pr/mckeesport-man-pleads-guilty-fbi-investigation-fraud-scheme

[13] DOJ. (2017, May 19). Three charged federally in Amazon fraud scheme. Retrieved from https://www.justice.gov/usao-sdin/pr/three-charged-federally-amazon-fraud-scheme-1

[14] Experian. (2018). The 2018 global fraud and identity report. Retrieved from https://www.experian.com/assets/decision-analytics/reports/global-fraud-report-2018.pdf

[15] Kount. (2018). Mobile payments and fraud: 2018 Report. Retrieved from https://info.kount.com/hubfs/White_Papers/Mobile_Payments_and_Fraud_2018_Report.pdf

[16] Rinsky, E. (2019). Five ecommerce and fraud trends to expect in 2019 [Web log post]. Retrieved from https://www.riskified.com/blog/five-ecommerce-fraud-trends-to-expect-in-2019/

[17] Merchant Marine. (2018). The rise of digital and mobile wallets: 2019 Global Usage Stats. Retrieved from https://merchantmachine.co.uk/digital-wallet/

[18] Rinsky, E. (2019). Five ecommerce and fraud trends to expect in 2019 [Web log post]. Retrieved from https://www.riskified.com/blog/five-ecommerce-fraud-trends-to-expect-in-2019/

[19] Nova, A. (2018). Bitcoin takes on cash, as more places accept the cryptocurrency. Retrieved from https://www.cnbc.com/2018/03/02/spending-cryptocurrencies-on-everyday-purchases-is-getting-easier.html

[20] Germain, J. (2019). Flexa launches crypto-based payment app. Retrieved from https://www.ecommercetimes.com/story/86014.html

[21] Sorrell, S. (2018). Future fraud: 3 dynamics changing fraud in 2019. Retrieved from Juniper Research website: https://www.juniperresearch.com/document-library/white-papers/future-fraud-3-dynamics-changing-fraud

[22] Experian. (2019, May 1). The State of Online Shopping Fraud. Retrieved from https://www.experian.com/blogs/ask-experian/the-state-of-online-shopping-fraud/

[23] UPS. (2019). Learn to Recognize Fraud. Retrieved from https://www.ups.com/us/en/help-center/legal-terms-conditions/fight-fraud/recognize.page

[24] RSA. (2019, April 10). Money Mules: The Critical Cash Out Service in the Fraud Supply Chain. Retrieved from https://www.rsa.com/en-us/blog/2016-04/money-mules-the-critical-cash-out-service-in-the-fraud-supply-chain

[25] Tech-Savvy Scammers Work to Con More Victims: 2018 BBB Scam Tracker Risk Report, 2018

[26] London Blue, April 2019 Update, UK-Based Multinational Gang Evolves Their Tactics, Targeting Asian Users and Spoofing Email Addresses. Retrieved August 8, 2019, from https://www.agari.com/cyber-intelligence-research/whitepapers/london-blue-april-2019.pdf

[27] DOJ. (2015, July 13). Six Nigerian Nationals Extradited from South Africa to Mississippi to Face Fraud Charges. Retrieved from https://www.justice.gov/usao-sdms/pr/six-nigerian-nationals-extradited-sout-africa-mississippi-face-fraud-charges

[28] [28] DOJ. (2016, May 17). Guilty Plea In International Internet Conspiracy Case. Retrieved from https://www.justice.gov/usao-sdms/pr/guilty-plea-international-internet-conspiracy-case

[29] USA. (2019). Report Scams and Frauds. Retrieved from https://www.usa.gov/stop-scams-frauds#item-35162

[30] WPF. (2015). EConsumer.Gov: Improved and updated multi-national consumer complaint website. Retrieved from https://www.worldprivacyforum.org/2015/10/econsumer-gov-improved-and-updated-multi-national-consumer-complaint-website/

[31] FTC. (2019). The FTC's Consumer Sentinel Network. Retrieved from https://www.ftc.gov/sites/default/files/attachments/consumer-sentinel-network/factsheet.pdf

[32] IC3. (2018). 2018 Internet Crime Report. Retrieved from https://www.ic3.gov/media/annualreport/2018_IC3Report.pdf

[33] Kevin McAleenan. (July 18, 2018). Testimony to U.S. Senate Committee on Finance

[34] Federal Register, (July 23, 2019). Vol. 84, No. 141, p. 35405

[35] Federal Register, (July 23, 2019). Vol. 84, No. 141, p. 35405

[36] FinCEN. (2018, June). FinCEN SAR Electronic Filing Requir. Retrieved from https://bsaefiling.fincen.treas.gov/docs/XMLUserGuide_FinCENSAR.pdf#page147

[37] D'Antuono, S. (2018, November 29). Combating Money Laundering and Other Forms of Illicit Finance. Retrieved from https://www.fbi.gov/news/testimony/combating-money-laundering-and-other-forms-of-illicit-finance

[38] FinCEN. (2018). Testimony of FinCEN Director Kenneth A. Blanco before the Senate Committee on Banking, Housing and Urban Affairs. Retrieved from https://www.fincen.gov/news/testimony/testimony-fincen-director-kenneth-blanco-senate-committee-banking-housing-and-urban

[39] FinCEN. (2018). Testimony of Thomas P. Ott, Associate Director, Enforcement Division, before the House Committee on Financial Services. Retrieved from https://www.fincen.gov/news/testimony/testimony-thomas-p-ott-associate-director-enforcement-division-house-committee

[40] DOJ. (2015, July 13). Six Nigerian Nationals Extradited from South Africa to Mississippi to Face Fraud Charges. Retrieved from https://www.justice.gov/usao-sdms/pr/six-nigerian-nationals-extradited-sout-africa-mississippi-face-fraud-charges

[41] DOJ. (2017, June 27). McKeesport Man Pleads Guilty in FBI Investigation into Fraud Scheme. Retrieved from https://www.justice.gov/usao-wdpa/pr/mckeesport-man-pleads-guilty-fbi-investigation-fraud-scheme

[42] DOJ. (2017, June 27). McKeesport Man Pleads Guilty in FBI Investigation into Fraud Scheme. Retrieved from https://www.justice.gov/usao-wdpa/pr/mckeesport-man-pleads-guilty-fbi-investigation-fraud-scheme

[43] DOJ. (2017, May 19). Three charged federally in Amazon fraud scheme. Retrieved from https://www.justice.gov/usao-sdin/pr/three-charged-federally-amazon-fraud-scheme-1

[44] DOJ. (2017, April 17). Man Admits Guilt in Stolen Identity Refund Fraud Scheme Using Hacked UPMC Employee Information. Retrieved from https://www.justice.gov/usao-wdpa/pr/man-admits-guilt-stolen-identity-refund-fraud-scheme-using-hacked-upmc-employee

[45] DOJ. (2017, June 27). McKeesport Man Pleads Guilty in FBI Investigation into Fraud Scheme. Retrieved from https://www.justice.gov/usao-wdpa/pr/mckeesport-man-pleads-guilty-fbi-investigation-fraud-scheme

[46] DOJ. (2017, May 19). Three charged federally in Amazon fraud scheme. Retrieved from https://www.justice.gov/usao-sdin/pr/three-charged-federally-amazon-fraud-scheme-1

[47] DOJ. (2015, July 13). Six Nigerian Nationals Extradited from South Africa to Mississippi to Face Fraud Charges. Retrieved from https://www.justice.gov/usao-sdms/pr/six-nigerian-nationals-extradited-sout-africa-mississippi-face-fraud-charges

[48] IC3. (2018). 2018 Internet Crime Report. Retrieved from https://www.ic3.gov/media/annualreport/2018_IC3Report.pdf

[49] RAND. (2018). Identifying Law Enforcement Needs for Access to Digital Evidence in Remote Data Centers. Retrieved from https://www.rand.org/pubs/research_reports/RR2240.html

[50] CSIS. (2018, July 25). Low-Hanging Fruit: Evidence-Based Solutions to the Digital Evidence Challenge. Retrieved from https://www.csis.org/analysis/low-hanging-fruit-evidence-based-solutions-digital-evidence-challenge.

[51] CSIS. (2018, July 25). Low-Hanging Fruit: Evidence-Based Solutions to the Digital Evidence Challenge. Retrieved from https://www.csis.org/analysis/low-hanging-fruit-evidence-based-solutions-digital-evidence-challenge.

[52] RCFL. (2019). Introduction to RCFLs. Retrieved from https://www.rcfl.gov/file-repository/rcfl_intro_042018.pdf/@@images/image/mini

[53] CSIS. (2018, July 25). Low-Hanging Fruit: Evidence-Based Solutions to the Digital Evidence Challenge. Retrieved from https://www.csis.org/analysis/low-hanging-fruit-evidence-based-solutions-digital-evidence-challenge.