SWIFT INSTITUTE

SWIFT INSTITUTE WORKING PAPER NO. 2016-003

SHARING INSIDER THREAT INDICATORS: EXAMINING THE POTENTIAL USE OF SWIFT'S MESSAGING PLATFORM TO COMBAT CYBER FRAUD

ELIZABETH M. PETRIE

CASEY EVANS

PUBLICATION DATE: OCTOBER 2, 2017

Sharing Insider Threat Indicators:

Examining the Potential Use of SWIFT's Messaging Platform to Combat Cyber Fraud

Elizabeth M. Petrie
Director, Cyber Threat Risk Management
Cyber Risk Management

Casey D. Evans, Executive-in-Residence
Program Director, Master of Science in Accounting
Kogod School of Business

Table of Contents

Acknowledgements ..... **iii**

Abstract ..... **iv**

1 Introduction **5**

2 Background **6**

2.1 Challenges to Information Sharing 6

2.2 U.S. Industry Threat Information Sharing Tools – Two Use Cases 7

3 Approach **10**

3.1 Insider Threat Activity 11

3.2 Behavioral Indicators of Fraud Activity 11

3.3 Recruiting an Insider 11

3.4 Fraud Rings 12

4 Findings **13**

4.1 Indicators of Insider Cashout Activity 13

5 Legal and Privacy Considerations **15**

5.1 Assumptions 16

5.2 Employee Monitoring 16

5.3 Employment Discrimination 17

5.4 Protection of Personal and Proprietary Information 17

5.5 Anti-Trust and Anti-Competitive Prohibitions 18

5.6 Additional Considerations 18

6 Development of the Insider Threat Report (ITR) **19**

6.1 Converting the Insider Threat Report into the SWIFT MT 998 Format 20

7 Next Steps **21**

Appendix A **22**

1 MT 998 Insider Threat Report **23**

1.1 Scope 23

1.2 Format Specifications 23

1.3 Specifications for field 77E 24

1.3.1 Network Validated Rules 24

1.3.2 Field Specifications 24

1.4 MT 998 Example 31

List of Figures

Figure 1: Reporting Bank 20
Figure 2: Insider Threat Activity 21
Figure 3: Point of Contact 21

Acknowledgements

The authors wish to thank the SWIFT Institute's research sponsorship program for funding this research and the expertise provided by SWIFT's technical group. Special recognition goes to Kogod Cybersecurity Governance Center (KCGC) Director Rebekah Lewis for the legal and privacy analysis published in this report, and KCGC Co-Founder William DeLone, for his oversight of the research methodology. The authors also wish to acknowledge Allison J. Bender for contributions on the development of an indicator sharing tool.

The views, opinions, and/or findings contained in this report are those of the authors and should not be interpreted as representing the official views or policies of Citi or American University.

Key Words

Cyber, Fraud, Intelligence, Indicators, Insider Threat, SWIFT, Information Sharing

Abstract

Cyber actors are operating under a shared services model giving them access to infrastructure, tools, targets and the ability to monetize their exploits. As a result, organizations across industries must enhance communication channels to share threat information in order to preempt cyber fraud schemes. This requires both an ability to identify the patterns of behavior that indicate cyber fraud activity is occurring and a platform for communicating potential threat information. This report focuses on identifying the patterns of behavior typically indicative of efforts by criminals to use insiders to cash out on fraudulent activity. The objective of this research is to explore the potential for organizations to use an existing telecommunication platform, such as SWIFT[1], to communicate cyber fraud threat information by establishing indicators of cashout behavior, which could warn of cyber fraud activity.

[1] According to https://www.swiftinstitute.org/about-us/, SWIFT, the Society for Worldwide Interbank Financial Telecommunications, is a member-owned cooperative, which provides a platform for messaging and standards for communicating for its members to conduct business operations.

1 Introduction

As companies across the globe move to a shared services model in adopting cloud technology, so too are cyber criminals. Lockheed Martin's Cyber Kill Chain[2] has been implemented across industries to study primarily nation-state sponsored cyber actors as they move through the seven stages of a cyber attack. By studying the behavior of the adversary at each stage of the attack, defensive programs can be customized to potentially stop an attack from advancing; however, there is limited sharing of the results of this behavior analysis as much of what is captured is considered either classified or proprietary. This research adopts the methodology of the Kill Chain to analyze the behavior of cyber actors committing cyber fraud in order to assess patterns of behavior that can be broken down into fraud indicators. The research will be based on a key assumption that cyber criminal actors are operating under a shared services model to outsource attack activity; therefore, patterns of behavior were assessed related only to those services that enable the cyber actor to monetize illicit activity, defined as cashout services. The outcome of our research is to advance the financial industry's ability to share threat information, which could prevent a cyber fraud event from occurring.

[2] Hutchins, Eric M., Michael J. Clopperty, Rohan M. Amin, "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains." Lockheed Martin Corporation. Accessed August 13, 2016 from http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf

2 Background

The evolution of technology not only enhances the ability of organizations to become more efficient and achieve higher rates of return, it also advances the cyber adversary's business model to achieve the highest gains in monetizing criminal activity with the lowest amount of risk. As a result, cyber actors are now outsourcing specific services required for successful schemes. When systems were not as complex as they are today, requiring a defense-in-depth approach to network security, cyber criminals could carry out attacks from start to finish. Today, cyber criminals need a sophisticated network of services to provide information on targets, such as network vulnerabilities; tools for attack, like root kits, botnets and customizable malware; secure communication channels; infrastructure to deploy an attack or obfuscate discovery by law enforcement; and most importantly, money transmitters and cashout services to monetize illicit gains.[3] Cyber actors' diversification of these set of services used in an anatomy of a cyber attack has forced organizations to change the way they are defending their networks by customizing defensive measures based on a study of the cyber actor's attack patterns against the network. However, these defensive measures are based on a narrow view of the cyber actor's attack activity as the configuration of the organization's network may preclude the observation of the cyber actor's full capabilities. That same cyber actor may be attacking another organization's network with similar, but perhaps enhanced, techniques because of the organization's structure. As a result, neither organization understands all of the cyber actor's tactics. These gaps in understanding are referred to as knowledge gaps and in order to address these gaps, organizations are coming together globally to exchange information in both public and private forums.

2.1 Challenges to Information Sharing

Considering the diverse cyber threat landscape and significant gap in time between when a network is breached and when a victim discovers the breach, organizations must do more to share information in a timely manner; however, organizations continue to struggle to overcome the challenge of information sharing for a number of reasons.

The Weapons of Mass Destruction ("WMD") Commission Report, published in March 2005, made a number of observations around information sharing by the United States Intelligence Community ("USIC"), which impacted the USIC's ability to properly assess if Iraq had weapons of mass destruction. A key finding was intelligence could not be shared with those who needed it because there lacked a centralized management system of intelligence information.[4] Without a centralized management function, processes did not exist to establish consistent thresholds for sharing intelligence, which took into account the risk management principles to balance protection of the source of information with the benefit of sharing. In addition, there was no uniform system available to transmit the intelligence using standards. The use of such standards to share information across one network would have allowed the collector of the intelligence to recall inaccurate intelligence reporting, or conversely, to send additional information to corroborate previous reporting. These standards would have given the consumer both a measure of confidence and reliability of the reporting they received. The benefit of having one intelligence information sharing network would have also resulted in the expansion of the information sharing environment.

In light of these observations and resulting recommendations, the USIC has erected a solid technical framework with uniform standards to enable effective intelligence information sharing; however, the fundamental key to the community's success has been the change in culture around information sharing. Prior to the 9/11 terrorist attacks, the culture of sharing was to share by exception in order to protect the sources and methods by which the intelligence was collected. Understanding how this culture led to the

[3] Paganini, Pierluigi. INFOSEC Institute (2013, August 07). "Cybercrime as a Service." Accessed August 17, 2016 from http://resources.infosecinstitute.com/cybercrime-as-a-service/

[4] WMD Commission (2005, March 31). "The WMD Commission Report: Final Report of the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction." Accessed April 9, 2017 from https://fas.org/irp/offdocs/wmd_chapter9.pdf, p.429

failures surrounding the 9/11 terrorist attacks, and implementation of a strong information sharing network, has since changed this culture.

It has been recognized by governments globally that cyber fraud represents a national security issue. As a result, cybersecurity is now embedded in government policy priorities, such as the U.S. Government's Cybersecurity National Action Plan. A key component of this plan is for Federal agencies to increase the availability of government-wide shared services for cybersecurity, building upon the 2015 Executive Order – Promoting Private Sector Cybersecurity Information Sharing. The 2015 Executive Order focuses on the ability of private companies, nonprofit organizations, and government agencies to share information on cyber incidents and risks.[5] The sharing of cyber threat information was supported in the 2015 Executive Order through the promotion of Information Sharing and Analysis Organizations to service critical infrastructure sectors. The Financial Services Information Sharing and Analysis Center ("FS-ISAC") was one of the first ISACs to be established in 1999 and has nearly 7000 members today.[6] Their mission is to share physical and cyber security threats and vulnerabilities among both private and public sector entities to protect the financial critical infrastructure.[7] Building upon the success of the FS-ISAC information sharing model, the Financial Systemic Analysis and Resilience Center ("FSARC") was established in October 2016 to focus on mitigating systemic risk to the U.S. financial system from cyber security threats through enhanced collaboration between industry and government entities.

However, despite efforts to increase information sharing among private, non-profit, and public organizations, there continues to be a lack of governance and a framework to streamline information exchanges and centralize information sharing management. In some cases, Structured Threat Information eXpression ("STIX") is used, which is a standardized, structured language for sharing cyber threat information. STIX is most often used with the Trusted Automated eXchange of Indicator Information ("TAXII"), an enabler of message exchanges and services.[8] The Automated Indicator Sharing ("AIS") capability created by the Department of Homeland Security uses STIX and TAXII to allow cyber threat indicators to be shared machine-to-machine. This capability enables organizations to expedite defense mechanisms to protect against the malicious indicators; however the reporting is not designed to give consumers the context surrounding the malicious use of the indicators. A reputational score is sometimes assigned, but the expectation is the consumer of the information will vet the indicators and decide what appropriate action should be taken.

Capabilities such as AIS demonstrate there are comprehensive standards available to exchange cyber threat information, yet these standards have not been widely adopted. Information sharing continues to primarily happen through list servs, working groups, phone calls and emails. The sharing of information is often tied to key individuals in an organization whose job it is to represent the company as external liaisons to both government and private working groups. Trust continues to be a critical factor to sharing information. Organizations need a framework under which they can share threat information without being held liable or risking another firm taking competitive advantage over exposing vulnerabilities of the reporting organization. In order to overcome these challenges of obtaining information that can fill knowledge gaps in how a cyber actor may commit fraud, and share this threat information with the broadest group possible, a framework for sharing must be adopted and thresholds for reporting established.

2.2 U.S. Industry Threat Information Sharing Tools – Two Use Cases

Intelligence Information Reports

[5] The White House (2015, February 13). "Executive Order -- Promoting Private Sector Cybersecurity Information Sharing." Accessed April 17, 2017 from https://obamawhitehouse.archives.gov/the-press-office/2015/02/13/executive-order-promoting-private-sector-cybersecurity-information-sharing
[6] Financial Sector-Information Sharing and Analysis Center. Accessed August 20, 2017 from https://www.fsisac.com/about/mission
[7] Ibid.
[8] Department of Homeland Security, United States Computer Emergency Readiness Team (US-CERT). Accessed April 15, 2017 from https://www.us-cert.gov/Information-Sharing-Specifications-Cybersecurity

One of the key findings in the 9/11 Commission Report was the failure to share information on terrorist activity, not just across U.S. intelligence agencies and between governments, but also within agencies themselves as silos existed.[9] To correct this failure, the culture of information sharing moved from a "need to know" to a "need to share" philosophy and a mechanism for sharing information throughout the intelligence community was implemented. This mechanism is the Intelligence Information Report ("IIR").

The FBI is one of the U.S. intelligence community agencies to have fully adopted the IIR as a mechanism for sharing raw, unevaluated information within the FBI as well as across intelligence agencies and law enforcement departments.[10] The IIR is formatted as a teletype message with standardized fields, disseminated to relevant stakeholders, such as the U.S. military, homeland defense departments, and even international agencies. In order to control for the quality of reporting in IIRs, standards have been created to mandate classification of the reporting, evaluation of the source of the information, key components of the reporting (i.e. the who, what, when, where, why and how principles of writing) and dissemination requirements. Implementation of standards for intelligence information reporting provides the consumer a level of confidence in the information and an understanding of what weight to assign its value. The true value of the IIR is to communicate information that in and of itself means very little; however, when added with other information, may reveal criminal activity.

The IIR also has the added benefit of serving as a vehicle for sharing reporting within an organization, as well as between intelligence agencies and law enforcement communities. This is through the customization of the distribution list. As a teletype, the IIR is transmitted using the IIR Dissemination System, networking multiple agencies together.[11] The use of one uniform system to send the communication also allows for recipients to customize alerts so that only IIRs pertinent to their area of responsibility are delivered to their mailbox, instead of creating an issue of information overload. Record management of IIRs is streamlined and centralized.

Suspicious Activity Reports

According to the Code of Federal Regulations, financial institutions are required to file Suspicious Activity Reports ("SARs") for the purpose of identifying suspicious transactions that may violate a law or be designed to circumvent the Bank Secrecy Act ("BSA").[12] Such transactions could be related to terrorist financing, financial crimes, cyber-events and cyber-enabled crime. SARs have a standard format with mandatory and discretionary fields; however, there are certain requirements for when SARs must be filed, regardless of the type of suspicious transaction being conducted. One of these requirements is for financial institutions to file on insider abuse involving any amount. The activity must be reported even if the insider only attempted the criminal act, yet no Federal criminal violation occurred.

Similarly, there is the requirement to file a SAR on a financial transaction if suspected to be part of a cyber event, even if the cyber event did not occur. The Financial Crimes Enforcement Network (FinCEN) issued an advisory in October 2016 calling attention to this requirement as the reporting aids law enforcement in combating cyber criminals and cyber enabled crimes. The *Advisory to Financial Institutions on Cyber-Events and Cyber-Enabled Crime* specifically requests the following information be provided: [13]

- Description and magnitude of the event
- Known or suspected time, location, and characteristics or signatures of the event

[9] National Commission on Terrorist Attacks (2004, July 22). "The 9/11 Commission Report." Accessed March 07, 2017 from https://www.9-11commission.gov/report/911Report.pdf, p.434
[10] American Civil Liberties Union (2010 June 10). "Federal Bureau of Investigation Intelligence Information Report Policy Implementation Guide." Accessed August 21, 2017 from https://www.aclu.org/sites/default/files/field_document/ACLURM006050.pdf p.1
[11] Ibid. p.4
[12] Cornell Law School, Legal Information Institute. "CFR-Title 12-Chapter 1-Part 21-Subpart B-Section 21.11-Suspicious Activity Report." Accessed April 17, 2017 from https://www.law.cornell.edu/cfr/text/12/21.11
[13] United States Department of the Treasury, Financial Crimes Enforcement Network (2016, October 25). "Advisory to Financial Institutions on Cyber-Events and Cyber-Enabled Crime." Accessed April 17, 2017 from https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2016-a005

- Indicators of compromise
- Relevant Internet Protocol (“IP”) addresses and their timestamps
- Device identifiers
- Methodologies used

In order to make the reporting as useful and relevant as possible, the SAR form includes fields to provide context to the suspicious transaction being recorded. SARs are required to be submitted using the BSA E-Filing System. This system implements the necessary requirements for secure transactions to occur and allows users to submit filings either individually or in batches. SAR filings are sent to FinCEN, which serves as the centralized management function for this reporting. FinCEN is able to perform analytics on the filings, which sometimes results in leads to law enforcement to open investigations or further support ongoing investigations. Trend analysis is also performed to determine concentrations of threat activity or changes in tactics. As financial institutions become more adept at identifying cyber events, this body of data will also grow and aid the community in understanding historical trends in activity over time.

3 Approach

In order to overcome the challenges of obtaining information that can fill knowledge gaps in how a cyber actor may commit fraud, and share this threat information with the broadest group possible, a standard for reporting must be adopted and thresholds for reporting established. The goal of this research is to establish indicators of insider cashout behavior and leverage an existing telecommunications platform to warn of insider threat activity that may be indicative of cyber fraud. Organizations worldwide recognize the well-established money laundering cycle for the purpose of investigating fraudulent acts. The United Nations Office on Drugs and Crime defines money laundering as a dynamic three stage process requiring placement, layering and integration of funds in order for the criminal to benefit from illegal profits without being identified.[14] The placement stage of the cycle is the point at which proceeds from the crime enter into the financial system. According to the U.S. Money Laundering Threat Assessment (2005), a financial institution is crucial in almost every money laundering typology for the criminal to hold or move funds.[15]

Although cyber criminals have diversified their techniques for conducting cyber fraud, they still require services to move and cashout their criminal proceeds. A typology on cashout services offered in the cyber underground does not exist. In order to build a body of reporting to identify when cashout activity is occurring, institutions must share information with one another on the cyber fraud activity that has been targeted against them. More specifically, sharing reporting on insider threat activity may contribute to a larger picture of cyber fraud activity happening across multiple institutions; however, insider threat information is highly sensitive as it could expose an organization's vulnerabilities. Defining indicators of insider cashout behavior which organizations can use to report to one another may preempt the fraudulent transfer of cash out of the financial system, thereby incentivizing organizations to share this information. Using this premise, the research conducted accounted for the following key assumptions, as noted below.

Key Assumptions:

- Insiders collude with individuals outside of the financial institution to perpetrate cyber fraud.
- The cashout phase for illicit cyber fraud activity is required for the insider to profit from the illicit cyber fraud activity.
- Indicators of insider cashout activity are indicative of illicit cyber fraud activity and not legitimate cashout activities.
- Financial institutions are willing to share threat intelligence on insider activities.
- Legal authorities allow for sharing of threat intelligence on indicators that may or may not be indicative of insider cyber fraud activity.

[14] United Nations Office on Drugs and Crime (2017). "The Money Laundering Cycle." Accessed March 07, 2017 from https://www.unodc.org/unodc/en/money-laundering/laundrycycle.html
[15] United States Department of the Treasury (2005, December). "U.S. Money Laundering Threat Assessment." Accessed March 07, 2017 from https://www.treasury.gov/resource-center/terrorist-illicit-finance/Documents/mlta.pdf

3.1 Insider Threat Activity

Many of the individuals who engage in fraudulent activity do not have a criminal history themselves. So why are they motivated to commit fraud? Their motives are best explained by Donald Cressey's Fraud Triangle. The fraud triangle originated from Donald Cressey's hypothesis:

> Trusted persons become trust violators when they conceive of themselves as having a financial problem which is non-shareable, are aware this problem can be secretly resolved by violation of the position of financial trust, and are able to apply to their own conduct in that situation verbalizations which enable them to adjust their conceptions of themselves as trusted persons with their conceptions of themselves as users of the entrusted funds or property.[16]

According to Cressey, there are three factors that must be present at the same time in order for an ordinary person to commit fraud: Pressure; Opportunity; and Rationalization.

Pressure is what leads an individual to engage in the fraudulent activity. For example, the individual has a financial problem and is unable to solve it through legitimate means. The illicit act is seen as a way to relieve the pressure created by the problem. The problem may stem from personal financial pressure to pay the bills, to support a vice (gambling addition, alcohol/drug abuse) or feed a desire for status symbols (new house, car, clothes, etc.). The problem may also be professional in nature, if the individual feels his/her job is in jeopardy due to layoffs or poor performance.

Opportunity defines the method by which the act can be committed. For example, a person may occupy a position of trust, which he/she may use to abuse the system and he/she perceives a low risk of being caught.

Rationalization is the way the individual justifies his/her conduct. Common rationalizations include thoughts that the act was harmless or temporary (e.g., the money would not be missed or would be paid back), and feelings of resentment or entitlement.

3.2 Behavioral Indicators of Fraud Activity

Individuals engaging in fraudulent activity will display certain behaviors outside of the norm. According to the Association of Certified Fraud Examiners' (ACFE) *2016 Report to the Nations*, it is common for occupational fraudsters to exhibit behavioral traits or characteristics while committing their schemes - such as living beyond their means, financial difficulties, unusually close association with customers, irritability, refusal to take vacation, and social isolation while committing their schemes.[17] Insider threats may be exposed by identifying suspicious behavior patterns. Understanding how these behavioral clues are linked to fraudulent conduct can help improve the chances of detecting fraud early and minimizing fraud losses.

An insider can be in a supervisory or non-supervisory role but will have a position in the organization that allows the employee to create, alter and terminate customer accounts. An insider will have financial and/or non-financial motivations to engage in fraud and may be recruited by an outsider or by someone they know personally.

3.3 Recruiting an Insider

Similar to posting a job opportunity in the local paper, cybercriminals will use the dark web to solicit bank employee credentials/system access in exchange for money. For example, hackers in Ireland offered

[16] Cressey, Donald R., (Montclair: Patterson Smith, 1973). "Other People's Money." p. 30.
[17] Association of Certified Fraud Examiners (2016). "Report to the Nations on Occupational Fraud and Abuse: 2016 Global Fraud Study." Accessed May 24, 2017 from https://s3-us-west-2.amazonaws.com/acfepublic/2016-report-to-the-nations.pdf, p. 68.

Apple employees up to 20,000 euros for valid login credentials.[18] If cybercriminals are unable to find an insider to help them gain outright entry to the bank's systems, they will recruit the insiders to perform more subtle tasks.

Insiders are also recruited by people they know personally or acquaintances who learned through the grapevine that they worked at a bank. According to a cyber fraud case profiled in *Trends in Organized Crime*, which involved hackers getting access to bank records with the help of employees of the bank, the bank employee would receive a financial reward for these activities.[19]

3.4 Fraud Rings

In the 2012 report, *Insider Fraud in Financial Services*, by researchers at Software Engineering Institute – Computer Emergency Response Team Division (CERT), which is considered a leading authority in the area of insider threat activity, insider fraud was defined as:

> Insider fraud is perpetrated by a malicious insider, which is a current or former employee, contractor, or other business partner who has or had authorized access to an organization's network, system, or data and intentionally exceeded or misused that access in a manner that negatively affected the confidentiality, integrity, or availability of the organization's information or information systems.[20]

To further narrow the definition of insider cashout activity, the insider activity must involve abuse of trusted access to compromise the confidentiality, integrity, or availability of an organization's data or its systems.

Insider cashout activity is part of broader cyber or fraud rings. For the purposes of this research, a ring is defined as two or more people colluding to conduct illicit activity. The Association of Certified Fraud Examiners (ACFE) also noted that over half the cases in the 2016 study had two or more people working together to perpetrate fraud. The analysis showed that the higher the number of people working together, the more costly to the victim organizations.[21] The Software Engineering Institute, Carnegie Mellon University, further found through analysis conducted on CERT's Insider Threat Data Set that incidents involving collusion had a longer duration than those committed by an individual insider.[22] Based on these findings, by reporting insider activity among financial institutions, the identification of a ring may be possible before significant losses due to cyber fraud are suffered as ring members may be colluding as employees of multiple financial institutions.

[18] Shead, S. (2016, February 09). "Hackers are offering Apple employees in Ireland up to €20,000 for their login details." Accessed August 12, 2016, from http://www.businessinsider.com.au/hackers-offering-apple-employees-in-ireland-euros-login-details-2016-2
[19] Leukfeldt, E.R. (2014) Cybercrime and social ties. Phishing in Amsterdam. In: Trends in Organized Crime. 17(4) 231-249. Trends in Organized Crime. 17. 231-249. https://www.researchgate.net/publication/280014116_Leukfeldt_ER_2014_Cybercrime_and_social_ties_Phishing_in_Amsterdam_In_Trends_in_Organized_Crime_174_231-249
[20] Software Engineering Institute – CERT Division (CERT). "Insider Fraud in Financial Services." Accessed December 7, 2016 from https://resources.sei.cmu.edu/asset_files/Brochure/2012_015_001_28207.pdf, p.3.
[21] Association of Certified Fraud Examiners (2016). "Report to the Nations on Occupational Fraud and Abuse: 2016 Global Fraud Study." Accessed May 24, 2017 from https://s3-us-west-2.amazonaws.com/acfepublic/2016-report-to-the-nations.pdf, p. 62.
[22] Software Engineering Institute, Carnegie Mellon University (2016, June 22). "The Frequency and Impact of Insider Collusion." Accessed August 20, 2017 from https://insights.sei.cmu.edu/insider-threat/2016/06/the-frequency-and-impact-of-insider-collusion.html

4 Findings

4.1 Indicators of Insider Cashout Activity

For purposes of this research, insider threat behavior was organized into the following categories.

Theft of Personally Identifiable Information (PII)

Theft of PII occurs when insiders maliciously act to steal bank customers' personal information. Examples of an indicator of theft of PII include an employee unnecessarily accessing and coping customer materials in a manner outside their responsibilities or emailing customer files to personal or web-based email accounts.

Theft of Trade Secrets

Theft of trade secrets occurs when bank employees are attempting to steal proprietary information from the bank with the intent to share it with criminals or competitors. Examples of theft of trade secrets include an employee staying at the office after hours and accessing sensitive data following termination notice or a laptop that has been wiped when returned after termination.

Cashout Activity

Cashout activity occurs when the insider is assisting cyber criminals with laundering their ill-gotten gains. Examples of cashout activity include an employee offering to aid placement of illicit funds on the dark web in exchange for payment; access to dormant accounts followed by sudden activity in the dormant accounts; and regularly changing customer account attributes.

We identified 54 indicators of insider behavior classified as indicative of theft of PII, theft of trade secrets, or cashout activity. These indicators were identified through an extensive review of professional and academic reports, white papers, and articles on fraudulent behavior and insider threats. Approximately 28% of the indicators identified matched only one category; the remaining 72% identified matched more than one category. Overall, 52% identified with all three categories.

In addition to identifying the category of insider activity, we also identified the source of the indicators such as network access data, customer account activity, email, human resource records, phone records, and internet browser history.

The list of 54 indicators, identified categories and source are provided below:

Insider Threat Indicators	Theft of PII	Theft of Trade Secrets	Cashout Activity	Source
Emails or IM with malicious language	X	X	X	Emails/Instant Messages
Mass emailing of sensitive company data to suspicious locations (personal email or cloud based storage)	X	X		Emails/Instant Messages
Complaints of hostile, abnormal, unethical or illegal behaviors	X	X	X	Hotline Logs
Chronic violation of organization policies	X	X	X	HR Records
Decline in work performance	X	X	X	HR Records
Terminations, layoffs and performance issues	X	X	X	HR Records
Network access data: web browsing history, network crawling, data hoarding, copying from internal repositories	X	X	X	Network Access Data
Employee staying at the office after hours after termination notice	X	X		Network Access Data
Communication with known high-risk personnel or external parties	X	X	X	Phone Logs

Insider Threat Indicators	Theft of PII	Theft of Trade Secrets	Cashout Activity	Source
Travel and entertainment data: violation of corporate policies	X	X	X	T&E Data
Travel to countries known for IP theft or hosting competitors	X	X	X	Travel Records
Offering to aid placement of illicit funds on the dark web in exchange for payment	X	X	X	Internet search
Emailing company files to personal or web-based email	X	X		Emails/Instant Messages
Use of USB storage devices	X	X		Network Access Data
Use of cloud based storage	X	X		Network Access Data
Printing critical data in bulk	X	X		Network Access Data
Sending scanned files to personal or web-based email (from copy machine)	X	X		Emails/Instant Messages
Installation of unauthorized software on work computers	X	X		Network Access Data
Inappropriately seeks or obtains information on subjects/customers not related to their work duties	X	X	X	Network Access Data
Interest in matters outside the scope of the employee's duties	X	X	X	HR Records/Hotline/WOM
Unnecessarily copies customer materials	X	X	X	Network Access Data
Unnecessarily copies computer code	X	X		Network Access Data
Unnecessarily accesses customer materials	X			Network Access Data
Unnecessarily accesses computer code	X	X		Network Access Data
Remotely accesses the network at odd times (while on vacation or during sick leave)	X	X	X	Network Access Data
Accesses restricted websites	X	X	X	Network Access Data
Conducts unauthorized searches	X	X	X	Network Access Data
Working odd hours without authorization	X	X	X	Network Access Data
Enthusiasm for working overtime and/or weekends	X	X	X	HR Records/Hotline/WOM
Short trips to foreign countries without legitimate reason	X	X	X	Internet search
Unexplained affluence	X	X	X	Internet search
Drop in performance and/or attendance	X	X	X	HR Records
Uncharacteristic comments made to co-workers	X	X	X	HR Records/Hotline/WOM
Sudden overuse of negative language in physical and electronic communications	X	X	X	Internet search
Expressing distaste with employer over social media	X	X	X	Internet search
Demonstrating ties to high-risk outside parties	X	X	X	Internet search
Irresponsible social media habits	X	X	X	Internet search
Accessing sensitive data after termination notice	X	X	X	Network Access Data
Taking pictures of intellectual property with personal phones/cameras	X	X		Employee Tip
Laptop that has been wiped when returned after termination	X	X	X	Hardware review
Employee staying at the office after hours prior to resignation		X		Network Access Data
Frequent or excessive access to accounts for high-net-worth or VIP customers			X	Network Access Data
Unnecessarily copies client lists		X		Network Access Data
Unnecessarily accesses client lists		X		Network Access Data

Insider Threat Indicators	Theft of PII	Theft of Trade Secrets	Cashout Activity	Source
Changing customer account statement mailing frequency to a longer period[23]			X	Network Access Data
An employee changed a customer address on an account unrelated to his/her duties			X	Network Access Data
Changing a customer attribute and returning it back within a specific time period[24]			X	Network Access Data
Searching for several dormant customer accounts[25]			X	Network Access Data
Transferring money from/to a dormant account[26]			X	Network Access Data
An account opened with a small deposit soon followed by large, electronically transferred deposits			X	Customer Account Activity
Account that suddenly begins to receive and send electronic funds transfers (EFTs) [27]			X	Customer Account Activity
A newly opened deposit account with an unusual amount of activity (i.e. account inquiries, big dollar or high number of incoming EFTs)[28]			X	Customer Account Activity
An account that receives incoming EFTs, then shortly afterward originates outgoing wire transfers or cash withdrawals approximately 10 percent less than the incoming EFTs[29]			X	Customer Account Activity
A foreign exchange student with a J-1 Visa opening a student account with an active volume of incoming and outgoing EFT activity.[30]			X	Customer Account Activity

5 Legal and Privacy Considerations

Note: The information in this document, including in this section regarding legal and privacy considerations, is not intended to provide and should not be construed as legal advice. Prior to implementing any activities described herein, individuals and companies should consult appropriate legal counsel and compliance personnel, and obtain a comprehensive legal analysis from their own legal counsel.

The indicator sharing messaging capability that we propose potentially implicates a number of legal issues spanning different areas of the law as well as established common principles and best practices related to the protection of privacy. Although numerous laws may apply to the proposed capability and the attendant legal risks could be substantial, we believe that participating entities can manage and significantly mitigate these risks by ensuring that various mechanisms and assurances are in place prior to implementation and usage. Below we provide a brief overview of these issues, including key assumptions that underpin our analysis as well as our thoughts on possible mechanisms for mitigating legal and privacy risks. As noted in "Next Steps," we will conduct a more in-depth review of these issues once the indicators are validated.

[23] Leuchtner, Tom. "4 internal frauds and how to spot them: Warning signs to spot, and technology that helps." *Banking Exchange*, 26 May 2011. Web. Accessed 09 Feb. 2017 http://www.bankingexchange.com/risk-management/item/2280-4-internal-frauds-and-how-to-spot-them

[24] *Id.*

[25] *Id.*

[26] *Id.*

[27] D'Alfanso, Steven. "Money Mule Targets: The Extremely Gullible and Financially Distressed" *Security Intelligence*. 09 Sept 2014. Web. Accessed 15 Dec. 2016 https://securityintelligence.com/money-mule-targets-the-extremely-gullible-and-financially-distressed/

[28] *Id.*

[29] *Id.*

[30] *Id.*

5.1 Assumptions

We based our assessment of potential legal issues at this stage of our research on several key assumptions. First, we have only considered U.S. law in this initial stage of analysis, and note that laws in other jurisdictions – including the EU's General Data Protection Regulation – may raise additional concerns and complexities. Second, we have assumed that the information collected and potentially shared via the proposed capability would be: i) limited to the 54 indicators identified in Section 4; ii) limited to information about the reporting entity's own employees and account holders; and iii) limited to information about U.S. citizens. Third, we assumed that the entities *collecting and disseminating* indicators through the capability would be limited to private U.S. financial sector companies that are already using the SWIFT messaging system in compliance with its terms of use and other requirements. Similarly, we assumed that the entities *receiving* indicators through the capability also would be limited to private U.S. financial sector companies using the SWIFT messaging system in compliance with all applicable requirements. Lastly, we assumed that the SWIFT messaging system itself, which will serve as the platform for the indicator sharing capability, is secured and maintained consistent with SWIFT's terms and conditions, personal data protection policy and other related documentation.

5.2 Employee Monitoring

Monitoring of employees' electronic communications and activities raises several legal and privacy issues, including prohibitions against the unauthorized interception of electronic communications or access to stored communications set forth in the Wiretap Act and the Stored Communications Act, both part of the federal Electronic Communications Privacy Act (ECPA). In addition, the Computer Fraud and Abuse Act (CFAA) also prohibits unauthorized computer access and use of information collected as a result of such access. Various state laws may also regulate employer monitoring of employees' electronic communications and activities. Entities who wish to share threat indicators that include the results of employee monitoring should ensure that they do not violate these prohibitions.

Many of these state and federal laws either do not apply or include specific exceptions if the employee has provided consent. For consent to be valid and sufficient, employers must provide notice that is clear, accurate and sufficiently detailed and broad to cover the various types of monitoring they use, the types of information collected, the purpose for the monitoring and the use of data once collected. If any of these factors change, employers should update the notice in order to ensure that consent is still valid and sufficient.

Employers can obtain explicit written consent to monitoring through a signed agreement or policy regarding acceptable use prior to an employee's use of any monitored devices. In addition to explicit consent, implied consent may be obtained by providing legally sufficient notice of the monitoring and of the fact that use of monitored devices, networks and systems constitutes implied consent to that monitoring. Notice mechanisms may include warning banners on all monitored devices (e.g., a popup window at login on computers or on browsers, preferably requiring affirmative employee acknowledgment) and appropriate policies, including the employee handbook and a corporate acceptable use policy. To be effective, these documents should be regularly updated to accurately reflect the employer's monitoring practices and should clearly state that employees' use of the device indicates their implied consent to monitoring. If monitoring practices change in a material way, employers should provide sufficient notice of the changes and employees should re-sign updated documents. These recommendations are also consistent with the principles of transparency, purpose specification and use limitation, several core tenets of the Fair Information Practice Principles that form the common foundation of privacy protections in the United States.

In addition to obtaining consent, entities that can demonstrate that they are acting in their capacity as a service provider when collecting and sharing threat indicators – working to protect and secure their own infrastructure and services – may not be subject to these prohibitions. However, demonstrating that the

entity is acting in its capacity as a service provider and establishing the full scope of its authorized actions in that capacity may be a more difficult and complex task than obtaining valid consent.

Related areas that may require more in-depth analysis include: i) monitoring of employee-owned devices ("BYOD"); ii) monitoring of private, password-protected employee accounts accessed from corporate devices, including social media accounts; and iii) monitoring of privileged communications (e.g., attorney-client, clergy, spousal).

5.3 Employment Discrimination

A number of laws protect employees from discrimination on the basis of their membership in a protected class (e.g., age, sex, race, religion, disability, citizenship, genetic information). In addition, guidance issued by the Equal Employment Opportunity Commission states that considering an individual's criminal history in making employment decisions may violate federal law. Although most likely not applicable, the Fair Credit Reporting Act and some comparable state laws also regulate the use of credit reports in employment decisions. To the extent that any of the information provided via the proposed messaging capability might be used to inform employment decisions, these protections and regulations should be considered.

As a general matter, employers collecting and disseminating fraud indicators can address these risks in part by ensuring that their practices do not target members of a protected class on the basis of their class membership and that their practices, even if not targeted, do not have a disparate impact on a particular class. When receiving fraud indicators, employers similarly should carefully consider whether they can use the indicators to inform employment decisions. In order to further mitigate these risks, employers should limit indicator collection, analysis, retention and sharing to information that is *necessary* to detection and prevention of insider fraud. These recommendations are also consistent with the Fair Information Practice Principles of data minimization, purpose specification and use limitation.

Related areas that may require more in-depth analysis include: i) the general permissibility of the use of fraud indicators in employment decisions, either at all and/or in the event that the indicators provide a clear indication of wrongdoing or misconduct; and ii) mechanisms for employees to access and correct inaccurate information collected about them for fraud detection purposes.

5.4 Protection of Personal and Proprietary Information

Several laws require corporate entities that collect, process or store personal and proprietary information – including information about employees or consumers – to protect that information in accordance with reasonable security standards and consistent with any representations they make regarding their information handling practices (e.g., in privacy policies, terms of use, etc.). "Security" in this context should be interpreted to include both technological solutions (e.g., encryption, access control, key management) as well as adequate policies, procedures and training practices. These requirements are also consistent with the Fair Information Practice Principles. Applicable laws may include federal statutes such as the Financial Services Modernization Act of 1999, also known as the Gramm-Leach-Bliley Act, which specifically applies to financial institutions, and the Federal Trade Commission Act, among others, and various state laws.

For data in transit via the SWIFT network, certain laws may require entities to verify security standards, either initially or on an ongoing basis, and relying on a terms of use or a contract clause alone may not suffice. In addition, entities using the SWIFT platform must still ensure that they properly provision and manage access to the platform. On either end of the transmission, entities should also ensure that they implement and maintain sufficient security measures to protect personal or proprietary information under the following circumstances: i) once the information is collected and before it is transmitted via SWIFT, if

they are the ones initially collecting; and ii) once the information is received, if they are on the receiving end of indicators via the SWIFT messaging platform.

Lastly, entities should also obtain sufficient assurances – by contract and potentially through independent verification measures – that any entities with whom they share indicators through the SWIFT platform will also properly secure the data.

5.5 Anti-Trust and Anti-Competitive Prohibitions

In 2000 and again in 2014, the U.S. Department of Justice's Antitrust Division and the Federal Trade Commission issued statements asserting that sharing of cyber threat information, in the normal course, would be unlikely to violate federal antitrust laws. However, the government's guidance also notes that the nature and detail of the information disclosed (including the fact that DOJ assumed cyber threat indicators are typically highly technical in nature) and the context in which entities share such information are highly relevant.

The fraud indicators that we've identified may be less technical than the "cyber threat indicators" previously considered by the government. Therefore, the content and purpose of the shared information will be important to ensuring that it does not raise any antitrust or anticompetitive (e.g., price fixing) concerns. Both sharing and receiving entities should ensure that the information shared is limited to only that which is necessary to preventing and detecting insider fraud. Price information or any other information that is not consistent with that purpose should not be shared.

5.6 Additional Considerations

In addition to the above issues, we note two other general areas of potential legal or privacy risk. First, in addition to federal and state statutes and regulations, employees or accountholders whose personal information is collected and shared could attempt to bring suit against entities engaged in indicator sharing for privacy torts such as intrusion upon seclusion, false light or public disclosure of private facts. Our initial analysis suggests that, in light of the requirements for these causes of action and existing case law, such claims may be unlikely to prevail. However, they could still be costly to litigate.

In addition, certain constitutional protections – including those enshrined in the First and Fourth Amendment – could be relevant in the event that a participating entity may be 'acting as an agent of the government,' even if they were not explicitly sharing indicators with any government entity. The applicability of these protections requires additional analysis which we have not undertaken. However, we note that many of the principles discussed above in the context of statutes and regulations, including notice, consent, purpose specification and use limitation, may be relevant to upholding these protections.

The above topics do not represent an exclusive list of potential legal and privacy issues associated with the proposed sharing capability, only those that we believe raise the most significant risks. In addition, at this point our analysis does *not* address the following facts and circumstances, which would be likely to introduce new issues: application of non-U.S. laws; collection, processing or sharing of any additional indicators not included in our initial list, or indicators about any individuals who are not U.S. citizens and customers or employees of the sharing entity; sharing of indicators with any entities other than authorized private U.S. financial sector SWIFT messaging partners, including any government or non-U.S. entities; and collection, processing or sharing of indicators for any purpose other than detecting and preventing fraudulent insider activity.

6 Development of the Insider Threat Report (ITR)

Leveraging elements from the format of the IIR and the SAR, we customized the Insider Threat Report (ITR) for banks to use to communicate instances of insider threat activity that could be precursors to cyber fraud. This report is designed to be completed by a member of the bank's internal investigations team or insider threat team. The fields included in the ITR are listed and described below. At this stage of our research, we did not designate which of the fields should be mandatory versus discretionary, potentially providing the reporting entity a higher degree of anonymity.

Reporting Bank

This section includes the legal name, address, city, state and zip code of the reporting bank.

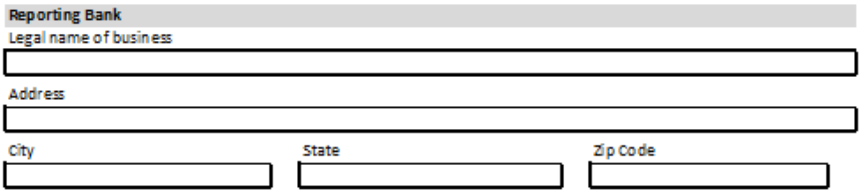

Figure 1: Reporting Bank

Insider Threat Activity

Type of threat

The submitter will choose the type of threat identified. The options are Theft of PII, Theft of Trade Secrets and Cashout Activity. The investigator will be permitted to pick one, two or all three categories of threats.

Threat action

The investigator will focus on the indicators of insider thereat activity in this section. For presentation purposes, the 54 indicators were culled down to 10. The 10 selected to be included on the Insider Threat Report are considered the most common among the indicators. The methods used to determine which indicators were most common included an extensive literature review of industry, trade, and general open-source publications; however the indicators have not yet been validated. The investigator may select all indicators that apply.

Severity of the threat

The goal of this section is to identify the financial and non-financial impact of the threat. The submitter will be asked to provide the date range of the threat and the type of account that was compromised. The submitter may select between corporate, individual or not applicable. The submitter will also have to provide the types of instruments that were used to facilitate the threat. Examples include but are not limited to wire transfers, trade instruments, structuring and money orders. The amount of financial loss, if any, must also be provided. If there are any other institutions affected by the threat, the submitter can provide the name of the institution. Actions taken to remediate or contain the threat, including notification to a regulator, can be described if desired.

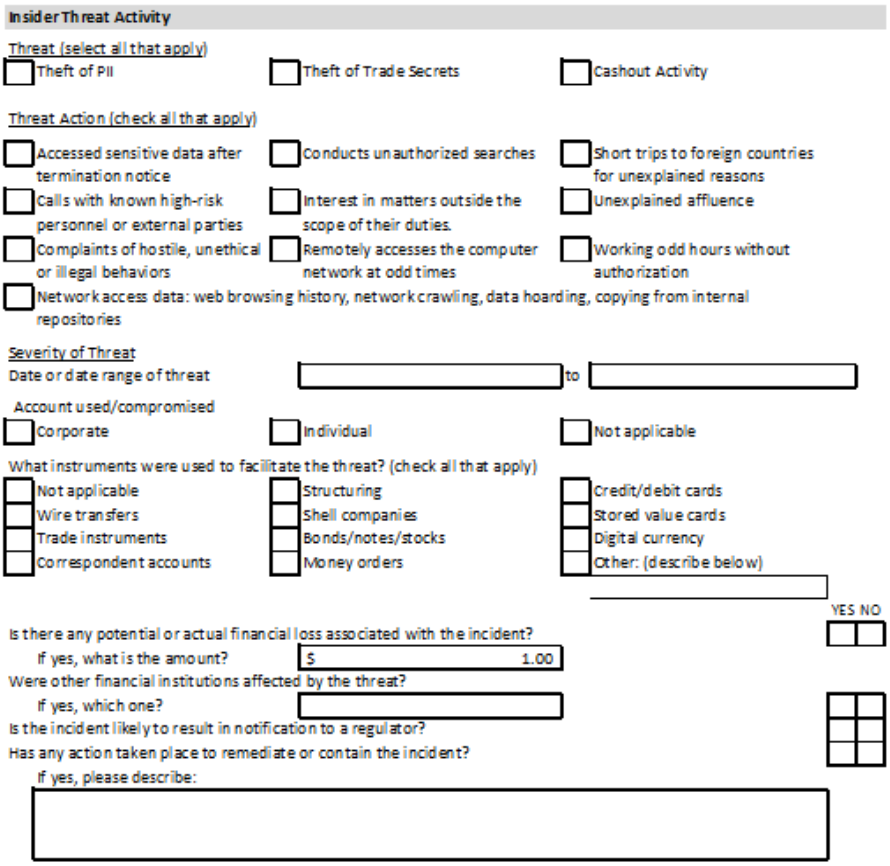

Figure 2: Insider Threat Activity

Point of Contact

This section includes the designated point of contact for the submitter and includes the report file date.

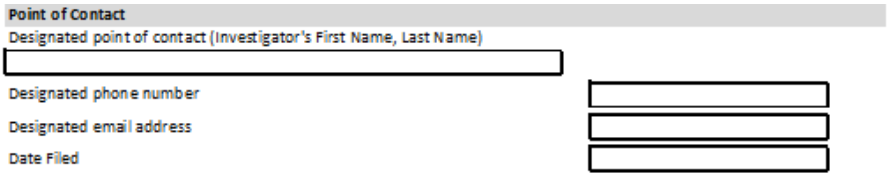

Figure 3: Point of Contact

6.1 Converting the Insider Threat Report into the SWIFT MT 998 Format

The objective of this research is to explore the potential for organizations to use an existing telecommunication platform, such as SWIFT, to communicate insider threat activity using our Insider Threat Report. After multiple meetings with experts at SWIFT, if this messaging proposal were to be implemented, the MT 998 report format would most likely be the appropriate format to communicate the information in the ITR. The MT 998 is a structured message that can be sent via the SWIFT network to SWIFT member banks, a sample of which can be found in Appendix A.

7 Next Steps

The findings from this research were presented at the *SWIFT Cyber Security 3.0 – Better Together* conferences hosted in London on March 30, 2017 and in Singapore on August 18, 2017. Feedback gathered from conference participants via polling indicated the community would like to see this research move into a pilot study. Effectiveness of conducting such a pilot would be contingent on the validation of all insider threat indicators presented in the research findings. In order to perform this validation, the indicators would be run against a body of known insider threat cases related to cyber fraud from FS-ISAC member organizations. To be considered valid, indicators would be ranked based on number of recurring instances they appear in the known body of reporting and an assessment performed on overall impact of the indicated behavior.

After validating, a sub-set of indicators would then be identified for use in a pilot based on capabilities to collect activity related to those indicators using existing tools. This would enable insider threat teams to do real time reporting of threat activity to the community. The remaining identified validated indicators could then be used by the investigative teams to issue reporting from insider threat cases in order to build a body of data on cashout activity. Indicators identified to be used in a pilot would then have to undergo a legal and privacy review to determine any constraints on sharing this type of information.

The next step of a pilot would require finalizing the message format for the ITR. Once finalized, pilot participants would fill out the ITR and begin exchanging the messages in a Closed User Group on the SWIFT platform.

If a pilot proved successful, expanding to include non-U.S. SWIFT member organizations could be assessed. An outcome of the pilot would also include definition of the procedures for writing and disseminating the ITR. As a pilot member, SWIFT would evaluate what standards would be required in order to implement an ITR message type and whether there is a broader community appetite for using such a mechanism for information sharing.

Appendix A

Insider Threat Report Message

Notional Message Type - SAMPLE

1 MT 998 Insider Threat Report

1.1 Scope

The Insider Threat Report message is the message a financial institution (branch/department) sends to either another branch/department of the same financial institution or to another financial institution reporting on information about a threat identified in the banking industry. It includes the details of the threat, the action(s) linked to it, the severity and assistance details from the reporting bank that is sending the Insider Threat Report.

1.2 Format Specifications

The MT 998 consists of two sequences:

- Sequence A Threat Activity is a single occurrence mandatory sequence and contains information linked to the threat identified
- Sequence B Assistance Details is a repetitive mandatory sequence and contains information of one or more contact person(s) that can be contacted regarding the Threat Activity described in Sequence A.

Status	Tag	Field Name	Content/ Options	No.
M	20	Transaction Reference Number	16x	UHB
M	12	Sub-Message Type	3!n (= 999)	UHB
M	77E	Proprietary Message	73x [n*78x]	UHB
Fields within field tag 77E:				
Mandatory Sequence A Insider Threat Activity				
----->				
M	23H	Category	4!c	1
-----|				
----->				
M	24H	Action	4!c	2
-----|				
Mandatory SubSequence A1 Severity				
M	30B	Date Range	6!n[/6!n]	3
----->				
O	25H	Account Type	4!a	4

-----|				
----->				
O	27H	Instruments	4!c	5
-----|				
End of SubSequence A1 Severity				
M	17C	Financial Loss Indicator	1!a	6
O	32T	Amount	3!a15d	7
----->				
O	56a	Other Affected Financial Institution	A, C or D	8
-----|				
M	17D	Regulation Notification Indicator	1!a	9
O	70B	Incident Remedial and/or Corrective Actions	4*70x	10
End of Sequence A Insider Threat Activity				
-----> Mandatory Repetitive Sequence B Assistance Details				
M	50a	Investigator	M, N or R	11
M	70H	E-mail	70x	12
M	30	Date	6!n	13
-----| End of Sequence B Assistance Details				

1.3 Specifications for field 77E

1.3.1 Network Validated Rules

C1 In Sequence A, when field 17C Financial Loss Indicator is “Y”, field 32T Amount must be present. (Error code(s): C56)

1.3.2 Field Specifications

1. Field 23H: Category

FORMAT

Option H 4!c (Code)

PRESENCE

Mandatory and repetitive in mandatory sequence A

DEFINITION

This field contains the category code to indicate the kind of threat reported.

CODES

One of the following codes must be used:

TPII	Theft of PII	The threat is the theft of Personally Identifiable Information
TTRS	Theft of Trade Secrets	The threat is the theft of Trade Secrets
CAOA	Cashout Activity	The threat is cashout Activity

EXAMPLE

:23H:TTRS

2. Field 24H: Action

FORMAT

Option H 4!c (Code)

PRESENCE

Mandatory and repetitive in mandatory sequence A

DEFINITION

This field identifies the type action involved in the threat.

CODES

One of the following codes must be used:

SENS	Sensitive Data	The threat action is accessing sensitive data after termination notice.
CALL	Calls	The threat action are calls with known high-risk (personnel or external parties).
BHVR	Behavior complaints	The threat action are complaints of hostile, unethical or illegal behaviors.
SENS	Sensitive Data	The threat action is accessing sensitive data after termination notice.
NDAA	Network Data Access	The threat action is access to network data: web browsing history, network crawling, data hoarding, copying from internal repositories.
SRCH	Searches	The threat action is conducting unauthorized searches.
OOSI	Out of Scope Interest	The threat action is interest in matters outside the scope of their duties.
REMA	Remote Access	The threat action is remotely accessing the computer network at odd times.
UFCT	Unexplained Foreign Country Trips	The threat action are short trips to foreign countries for unexplained reasons.
UAWH	Unauthorized Working Hours	The threat action are odd working hours without authorization.

		data: web browsing history, network crawling, data hoarding, copying from internal repositories.
UXAF	Unexplained affluence	The threat action is unexplained affluence.

EXAMPLE

:24H:NDAA

3. Field 30B: Date Range

FORMAT

Option B 6!n[/6!n] (StartDate)/(EndDate)

PRESENCE

Mandatory in mandatory subsequence A1

DEFINITION

This field contains the date range of the threat by indicating the start date and end date, if known, of the threat.

NETWORK VALIDATED RULES

Date must be a valid date expressed as YYMMDD (Error code(s): T50).

USAGE RULE

When subfield EndDate is not present, it is assumed that the treat is still active.

EXAMPLE

:30B:170322

4. Field 25H: Account Type

FORMAT

4!a (Code)

PRESENCE

Optional and repetitive in mandatory subsequence A1

DEFINITION

This field contains the account type used or compromised in the threat.

CODES

One of the following codes must be used:

CORP	Corporate account	A corporate account was used/compromised.

INDV	Individual account	An individual account was used/compromised.

EXAMPLE

:25:CORP

5. Field 27H: Instruments

FORMAT

Option H	4!a[/30x]	(Code)(Additional Information)

PRESENCE

Optional and repetitive in mandatorysub sequence A1

DEFINITION

This field contains the instrument used to facilitate the threat .

CODES

One of the following codes must be used:

WITR	Wire Transfers
TRIN	Trade Instruments
CRPA	Correspondent accounts
STRC	Structuring
SHCO	Shell Companies
BNSS	Bonds/notes/stocks
MNOR	Money Orders
CDCA	Credit/debit cards
SVCA	Stored Values cards
DICU	Digital Currency
OTHR	Other

NETWORK VALIDATED RULES

When field 27H is repeated, the same code word must not be present more than once with the exception of OTHR. The code word OTHR may be repeated (Error code(s):).

When the code OTHR is used, subfield Additional Information is mandatory (Error code(s):).

EXAMPLE

:27H:BNSS

6. Field 17C: Financial Loss Indicator

FORMAT

Option H	1!a	(Indicator)

PRESENCE

Mandatory in mandatory sequence A

DEFINITION

This field indicates if there was potential or actual financial loss associated with the incident .

CODES

One of the following codes must be used:

N No No financial loss.

Y Yes There was or could be financial loss.

7. Field 32T: Amount

FORMAT

Option T 3!c15d (Currency)(Amount)

PRESENCE

Conditional in mandatory sequence A

DEFINITION

This field indicates the amount of financial loss associated with the incident.

NETWORK VALIDATED RULES

Currency must be a valid ISO 4217 currency code (Error code(s): T52).

The integer part of Amount must contain at least one digit. A decimal comma is mandatory and is included in the maximum length. The number of digits following the comma must not exceed the maximum number allowed for the specified currency (Error code(s): C03,T40,T43).

8. Field 56a: Other Affected Financial Institution

FORMAT

Option A [/1!a][/34x] (Party Identifier)
4!a2!a2!c[3!c] (Identifier Code)

Option C /34x (Party Identifier)

Option D [/1!a][/34x] (Party Identifier)
4*35x (Name and Address)

PRESENCE

Optional and repetitive in mandatory sequence A

DEFINITION

This field indicates another financial institution affected by the threat.

NETWORK VALIDATED RULES

Identifier Code must be a registered financial institution BIC (Error code(s): T27,T28,T29,T45).

Identifier Code must be a financial institution BIC. This error code applies to all types of BICs referenced in a FIN message including connected BICs, non-connected BICs, Masters, Synonyms, Live destinations and Test & Training destinations (Error code(s): C05).

9. Field 17D: Regulation Notification Indicator

FORMAT

Option H 1!a (Indicator)

PRESENCE

Mandatory in mandatory sequence A

DEFINITION

This field indicates if the incident is likely to result in a notification to a regulator.

CODES

One of the following codes must be used:

N No

Y Yes

10. Field 70B: Incident Remedial and/or corrective actions

FORMAT

Option B 4*70x (Narrative)

PRESENCE

Optional in mandatory sequence A

DEFINITION

This field indicates a narrative description of actions taken place to remediate or contain the incident.

11. Field 50a: Investigator

FORMAT

Option M 4!a2!a2!c[3!c] (Identifier Code)
Option N4*35x (Name and Address)
Option R4*(1!n/33x) (Number)(Name and Address Details)

PRESENCE

Mandatory in mandatory and repetitive sequence B

DEFINITION

This field indicates the designated point of contact for the investigation.

CODES

In option R, Number must contain one of the following values:

1	Name of the Investigator	The number followed by a slash, '/' must be followed by the First name and Last name of the investigator.
2	Address Line	The number followed by a slash, '/' must be followed by an Address line (Address Line can be used to provide for

		example, street name and number, building name or post office box number).
3	Country, Town	The first occurrence of number 3 must be followed by a slash, '/', the ISO country code and, optionally, additional details that are preceded by a slash '/'. Other occurrence(s) of number 3 must be followed by a slash '/' and the continuation of additional details. Additional details can contain town, which can be complemented by postal code (for example zip) and country subdivision (for example, state, province, or county). The country code and town should, preferably, indicate the country and town of residence.

NETWORK VALIDATED RULES

Identifier Code must be a registered BIC (Error code(s): T27,T28,T29,T45).

In option R, for subfields (Number)(Name and Address Details):

• The first line must start with number 1 (Error code(s): T56).

• Numbers must appear in numerical order (Error code(s): T56).

• Number 2 must not be used without number 3 (Error code(s): T56).

• The first occurrence of number 3 must be followed by a valid ISO country code (Error code(s): T73).

USAGE RULES

At least the name or the BIC of the investigator is mandatory.

12. Field 70H: E-mail address

FORMAT

Option H	70x	(Narrative)

PRESENCE

Mandatoryl in mandatory and repetitive sequence B

DEFINITION

This field indicates a designated e-mail address of the investigator.

USAGE RULES

The character @ is not part of the x-character set on the SWIFT FIN network. Therefore, SWIFT recommends the use of the hexadecimal EBCDIC code (7C) for this character, preceded by two question marks (??) as an escape sequence. For example: Jack.Johnson@gmail.com will be Jack.Johnson??7Cgmail.com

13. Field 30: Date

FORMAT

No letter Option 6!n (Date)

PRESENCE

Mandatory in mandatory and repetitive sequence B

DEFINITION

This field contains the date of when the threat was filed.

NETWORK VALIDATED RULES

Date must be a valid date expressed as YYMMDD (Error code(s): T50).

1.4 MT 998 Example

Sender BANKUS33BOS

MT 998

Receiver BANKUS33CAL

:20:THREATREPORT170328

:12:999

:77E::23H:CAOA

:24H:CALL

:24H:OOSI

:24H:UAWH

:30B:170101/170327

:25H:INDV

:27H:WITR

:27H:MNOR

:27H:CDCA

:17C:Y

:32T:USD5000,

:17D:N

:70B:Employee dismissed

:50R:1/Emma Jackson

3/US/Boston

:70H:Emma.Jackson??7Caol.com

:30:170327