CYBER THREATS
Carnegie Mellon’s Computer Emergency Response Team (CERT) Resilience Management Model defines a threat as “the combination of a vulnerability, a threat actor, a motive, and the potential to produce a harmful outcome.” In the present geopolitical climate, the United States financial services sector is an attractive target for nation-states, terrorists, organized crime, hacktivists, and cybercriminals. Motives driving threat actors span the gamut; they could be for political or ideological reasons, or for retaliation or financial gain. While these threat actors leverage a range of malware variants and exploit both known and unknown vulnerabilities, one could argue they currently have the advantage in the cyber threat landscape.

One of the most effective ways to mitigate this situation is for financial institutions to share information relating to these cyber threats. However, the anecdotal evidence is that financial institutions are not using the available information sharing mechanisms to the maximum extent. This article will explore the reasons why this situation exists and what might be done to increase the sharing of cyber-related information in the financial industry.

Information Sharing and Section 314 of the USA PATRIOT ACT

After the 9/11 terrorist attacks, the U.S. Government saw that information sharing of valuable intelligence needed to increase to counter threats. Thus, in 2001 Congress enacted the USA PATRIOT Act to provide, among other things, mechanisms to facilitate the exchange of information in the financial industry. Operationally, the tools in place to facilitate public-private sector information sharing on money laundering and terrorist financing fall under Sections 314(a) and 314(b) of the USA PATRIOT Act. Section 314(a) allowed the Secretary of the Treasury to adopt regulations to encourage regulatory authorities and law enforcement to share information with financial institutions regarding individuals, entities, and organizations engaged in terrorist acts or money laundering. Section 314(b) permits financial institutions, upon providing notice to the United States Department of the Treasury, to share information with one another to identify and report to the federal government activities that may involve money laundering or terrorist activity.

Most importantly, this provision offers financial institutions “safe harbor” for the voluntary sharing of information, with a goal of assisting in countering money laundering and terrorist financing activities. Safe harbor is defined by FinCEN as protections from liability when sharing this type of information, and participating in 314(b) provides the following benefits:

- Alerts participating institutions of its customers’ suspicious activity;
- Facilitates informed decision making due to having a more accurate picture of activity;
- Aids in filing more comprehensive SARs;
- Identifies more illicit activity and complexity in various typologies;
- Assists in gathering additional information on transactions and customers which were previously unknown.

Four years after the enactment of the USA PATRIOT Act, then-President George W. Bush directed intelligence agencies to “develop high-level information sharing performance measures,” to encourage this desired activity. The value of this type of collaboration is not limited to counter-terrorism efforts. Much like the “near universal agreement”4 in the post 9/11 aftermath,5 that information sharing was needed to combat terrorism, a similar realization is emerging among banking professionals that greater information sharing on cyber threats is necessary to tackle a host of cyber-enabled financial crimes. Any crime that exists in the physical realm can be much more easily occur in—or be facilitated by—the virtual one. These cyber-enabled crimes can range from terrorism, sanctions evasion, human trafficking, extortion, drug trafficking, child exploitation, market manipulation, to fraud. Cyber-enabled crimes leverage shell corporations, well-developed mule networks, virtual currencies, peer-to-peer payment systems, and money laundering strategies to move ill-gotten funds—just like traditional organized crime networks do.

The impact of cyber-enabled crimes on our society, financial stability, reputation, and bottom line are astounding. At the heart of the matter, financial institutions may not necessarily know whether its visibility in a fraud or money laundering transaction is derived from cyber-enabled origins. For example, law enforcement feed-

Does your organization have plans to invest in more computer technology over the next few years? More than likely the answer is “yes,” however, does everyone understand how this will create more vulnerabilities for tech savvy criminals to threaten your institution?
Cyber-enabled Financial Crimes and 314(b)
Can financial institutions use Section 314(b) of the USA PATRIOT Act to share information relating to cyber-enabled financial crimes? According to the FinCEN FAQs published in conjunction with the FinCEN Advisory in October 2016, the answer is a resounding “Yes.” However, experience demonstrates banks are still reluctant or ultra-cautious in utilizing Section 314(b) in cases involving cyber events and cyber-enabled crime information.

Why does this attitude prevail, even after FinCEN has clearly expressed support for such sharing? Lester Joseph, head of Wells Fargo’s Global Financial Crimes Intelligence Group and former Principal Deputy Chief of the Department of Justice’s Asset Forfeiture and Money Laundering Section believes there are several options which explain this reluctance. First, even with the green light from FinCEN, there is some uncertainty as to what kind of cyber information can or should be shared. Second, banks traditionally have used section 314(b) on a transactional basis, meaning that banks use the provision to query other banks about financial transactions. However, if the only information to be shared involves cyber information, such as a kind of malware, banks often do not consider using 314(b). Moreover, it is not entirely clear whether 314(b) covers this kind of information. Section 314(b) refers to information “regarding individuals, entities, organizations, and countries suspected of possible terrorist or money laundering activities.”

Nathan Sales notes, “[I]nformation sharing can reduce the likelihood of catastrophic intelligence failures.” The Financial Services Information Sharing and Analysis Center (FS-ISAC), which is the most widely adopted cyber threat information sharing program in the U.S. financial sector, unfortunately has restrictions and gaps within cyber-enabled financial crimes space relating to legal and privacy restrictions on sharing of Personally Identifiable Information (PII). Ultimately, this indicates the information sharing mechanism that offers financial institutions the greatest protections and the widest range of datasets to include PII is 314(b).

FinCEN is quite clear that if 314(b) participants suspect transactions may involve proceeds of specified unlawful activities (SUAs) under money laundering statutes, they may share this information with safe harbor protections. Examples of SUAs listed in 18 U.S.C. §§ 1956 and 1957 are explicitly defined and broad enough in scope to cover cyber-enabled financial crimes, whether at the hacking, fraud, or money laundering phase. (See Table 1.)

FS-ISAC & NCFTA—Alternatives in Sharing Cyber Threat Information
The Financial Services Information Sharing & Analysis Center’s (FS-ISAC’s) mission is “to help assure the resilience and continuity of the global financial services infrastructure and individual firms against acts that could significantly impact the sector’s ability to provide services critical to the orderly functioning of the global economy” (www.fsisac.com/about/mission). FS-ISAC accomplishes this objective by continual cyber threat information exchange between its 7,000 members and using its sharing capability to distribute threat alerts and other critical information to its members across the world to help the sector prepare for, respond to, and mitigate risks and threats. FS-ISAC is a member-owned, non-profit organization created in response to Presidential Directive 63 to open communication channels between public and private sectors to share important security information to help protect U.S.-critical infrastructure. It is used by the global financial industry as a resource to share timely, relevant, and actionable physical and cyber threat and incident information, but not PII.

Another avenue for information sharing on cyber threats is the National Cyber-Forensics Training and Alliance (NCFTA). The NCFTA (www.ncfta.net) is a non-profit dedicated to addressing, mitigating, and neutralizing global cybercrime threats. The NCFTA operates in a concerted effort with law enforcement, private industry, and academia by sharing real-time information and working as an early-warning system to pass information quickly to its members. Through its partnership with many private-sector members, Carnegie Mellon University’s CERT, and the FBI’s Internet Crime Complaint Center (IC3), the free-flow exchange of threat intelligence assists investigation and prosecution of cybercriminals worldwide.

Challenges in using 314(b) in the Cyber Realm

1. SILOS. Cybercriminals, also known as “threat actors” in the information security world, count on financial institutions having a silo mentality to evade detection and prosecution. It is not uncommon for a cybercriminal scheme to cross several financial institutions, countries, and typologies. U.S. financial institutions, under the Bank Secrecy Act, currently file Suspicious Activity Reports (SARs) to the U.S. Financial Intelligence Unit (FIU), which is the Financial Crimes Enforcement Center (FinCEN). These reports contain valuable data for U.S. law enforcement agencies, the U.S. Intelligence Community and its partners as financial institutions collect actionable data and intelligence pursuant to the PATRIOT Act, as well as provide transactional reporting and analysis to SAR consumers. When we share information to identify the more extensive network, richer datasets become available to law enforcement to neutralize bad actors.
2. **Speed.** Cyber-financial crimes occur rapidly, and the delay or absence of information sharing allows cybercrime to continue unfettered. Faster information sharing positions financial institutions better to prevent cyber-enabled fraud, money laundering, and terrorist financing, as well as increase fraud recovery rates.

3. **Voluntary participation.** (www.fincen.gov/sites/default/files/shared/314bfactsheet.pdf). If financial institutions have not notified FinCEN of their intent to share information under 314(b), any external financial institutions that have valuable information about cyber cases involving the non-participating, end up with data that is not actionable. Participating in 314(b) information sharing serves to strengthen the industry immune system by shutting down avenues to launder proceeds of crime and providing more robust and accurate SAR reporting to FinCEN.

### Benefits and Use Cases for 314(b) Cyber Information Sharing

Financial institutions’ fraud prevention programs work vigilantly to keep threat actors from even accessing bank systems and customer accounts. Despite this, the combination of social engineering, malware, and systems vulnerabilities provide a way for accounts to be compromised. Financial institutions battle prolific cyber-enabled frauds such as synthetic identity fraud, business email compromise, romance fraud, and hacking incidents relating to payment systems.


International cybersecurity expert Dr. Shane Shook notes critical cyber threats and vulnerabilities which uniquely affect the financial sector:

- In the absence of national cybersecurity regulations, third-party payment processors and Real Time Gross Settlement (RTGS) providers reveal vulnerabilities in U.S. financial institutions and payment systems infrastructure.
- Cybercriminals and nation states seeking to gain funds to effect geopolitical outcomes will continue to target the U.S. banks, the securities market, and trading or technical platforms, which could also damage the U.S. economy and stability.
- Nation states will continue to target identified vital persons in financial institutions to uncover non-public information and trade secrets to gain or increase competitive edge, global standing, and leverage.

Faced with cybercriminal underground markets that are flooded with consumer PII (as a result of a series of massive data breaches and hacking incidents), fraud filters leveraged by financial institutions work overtime to stem losses. A challenge in the synthetic identity fraud environment is that there is no actual “victim” which self-reports or notifies law enforcement, which places the burden of identification squarely on the shoulders of the collective corporations in the financial services industry.

Synthetic identity is achieved when fraudsters combine pieces of legitimate data (such as a Social Security Number) with fabricated data (such as a false name), and merge it with an address belonging to yet another individual. Synthetic identity fraud is a daunting issue for consumers, corporations, and financial crime fighters; according to the Federal Trade Commission, synthetic identity fraud accounts for nearly 74 percent of all fraud losses by United States businesses, and over 88 percent of all identity theft incidents.

In the Journal of Financial Crime, P. Gottschalk states in the chapter “Theories of Financial Crime,” that key drivers are represented in what is termed “the fraud triangle,” or the notion that the risk of fraud arises when three factors are present: opportunities, incentives or pressures, and rationalization. Interaction among these elements differ by financial crime type, and in some cases from country to country. Insights as to why, are dependent upon the:

- Classification of the threat actor’s role (organized crime, insider);
- Environment;
- Degree of criminality in the countries where the fraud occurs;
- Geopolitical climate; and
- Likelihood of getting caught and prosecuted.

Synthetic identity fraud is problematic for credit monitoring services to detect, in part due to credit history entries appearing at credit bureaus only when there is an exact match of a consumer’s name and other PII.

A white paper published by ID Analytics notes a drastic increase in new social security numbers (SSNs) following the 2011 Social Security Administration implementation of randomized SSNs. While this move by the SSA was meant to protect consumers, unfortunately it created challenges for the financial services industry and its third-party providers to detect which SSNs are fraudulent. Thus, financial institutions leveraging 314(b) for sharing information connected to cyber-enabled financial crimes such as synthetic identity fraud, are highly likely to improve fraud prevention and the institutional bottom line significantly.

### FININT Value and the Regulatory Environment

The underlying framework in which threat actors’ financial activities operate, is the U.S. financial system. In this framework, there is a delicate balance between U.S. financial institutions’ obligations to their regulators and the financial intelligence (FININT) value delivered to the intelligence community and law enforcement. Regulators want to ensure programs are run adequately, and that reporting occurs on time.

While it is important to note that the safe harbor does not include sharing information across international borders, there are many technical indicators which can be shared and subsequently serve as dynamic investigational pivot points. Many of these are in the October 25, 2016 FinCEN Advisory:

- IP addresses with timestamps;
- User agent strings;
- Device IDs;
- Virtual wallet information;
- Indicators of compromise;
- Malware hashes, and more.
Going beyond technical indicators, institutions could share information relating to:

- Synthetic identity fraud;
- Mule accounts;
- Email addresses;
- Hone numbers, and
- Physical addresses.

In due course, including more technical data in SAR reporting assists law enforcement in compiling the whole picture, and it also serves as a way for individual institutions to identify technical indicators and networks of repeat offenders which may not be in the scope of fraud operations. Currently, college students and romance-fraud victims represent a good portion of the steady pipeline of mule accounts which are subsequently used to launder proceeds of cyber-crime around the world.

**Doing the Right Thing**

This topic is highly relevant to all stakeholders affected by threat actors operating in the virtual environment; financial institutions, information sharing entities, regulators, law enforcement, and the intelligence community. Like many mission-oriented fields where leadership outcomes have a societal impact, leadership in information sharing within the financial crimes and compliance community is of critical importance. Dr. Charles VanDeeper notes in his writings on intelligence and decision-making processes, that our society is in an age of “an abundance of information” and “daily access to advanced information technologies.”

The challenge is clearly not a lack of technology or expertise. Instead, it is in the synthesizing and sharing of information to render it valuable and actionable. In such instances, fraud investigations teams work hard to recover stolen funds to return them to rightful owners. Fraud investigators often labor under tight time constraints, with conflicting data presented to them. Where these funds are not able to be recovered, complex money laundering schemes have been identified which muddy the trail to the final beneficiary of cyber crimes. AML investigators, on the other hand, often look at this data through a different lens; they are excellent at uncovering hidden patterns and networks. Through yet another lens, information security teams can look at technical data and tell what the logs mean that are connected to an account or network activity—highlighting the absolute importance of fraud, AML, and information security teams working together. Each unit has essential skills and datasets needed to combat these threats, which ultimately might need to be shared with other financial institutions connected to a particular scheme.

What are the high-level basics needed to get started in sharing cyber-enabled financial crimes information?

1. Register with FinCEN Secure Information Sharing System (SISS) and comply fully with all requirements and operational practices.
2. Designate a 314(b) point of contact in your institution.
3. Break down operational silos in your institution and open up 314(b) to fraud, AML, and information security team members.
4. Ensure the entity you wish to share information with is a 314(b) participant.
5. Share.

**Finding Common Ground**

Finding common ground in the areas of information security, fraud, and AML use cases and datasets that make it possible to connect the dots in criminal activity. As technology and artificial intelligence grow ever more sophisticated, it will be teams and organizations who work together (and make sense of the noise), that emerge successful in fighting financial crimes. When companies share data relating to threat actors and the accounts they cultivate (for fraud, money laundering, or terrorism), the best opportunities for identifying and reporting threat actors emerge. Evolving to address cyber threats safely and efficiently should yield actionable intelligence shared in a rapid, scalable, and secure manner which can reduce risk and losses for financial institutions, and assist law enforcement in a more meaningful way.

**ABOUT THE AUTHOR**

**KELLEY CHAMBERLAIN, CAFP**, leads a team within Wells Fargo’s Global Financial Crimes Intelligence Group focusing on cyber-enabled financial crimes. The primary mission of the team is to provide strategic and tactical intelligence reporting and collaborative partnerships to combat financial crimes. Prior to joining Wells Fargo, Ms. Chamberlain was an Associate at Booz Allen Hamilton supporting cyber threat intelligence, financial intelligence, and open source intelligence endeavors. Ms. Chamberlain is a veteran of the United States Marine Corps. Additionally, she has held FINRA Series 7 and Series 66, and COMPTIA Security+ certification, and is currently pursuing a Master of Science in Applied Intelligence.

All views expressed by Ms. Chamberlain in this publication are her personal views and do not necessarily reflect the views of Wells Fargo Bank, N.A., its parent company, affiliates and subsidiaries.

**Endnotes**

10. Author’s personal interviews with Dr. Shane Shook during 2017 to 2018.