INTELLIGENCE AND
NATIONAL SECURITY ALLIANCE

POSITION PAPER

February 2018

Improving Information Sharing on Suspected Financial Fraud

Broadening Interpretation of the USA PATRIOT Act to Enhance National Security

Prepared by
THE INSA FINANCIAL THREATS COUNCIL

EXECUTIVE SUMMARY

Congress drafted Section 314 of the USA PATRIOT Act (the "Act") explicitly to incentivize financial institutions to work with law enforcement agencies and each other in support of the common goal to deter money laundering and terrorist financing. As written, Section 314(b) permits financial institutions to share information *only* in instances of suspected terrorism and money laundering. Thus, many banks in the United States are unable to share information under the 314(b) safe-harbor program when they suspect customers' funds are derived from other fraudulent activities. This is a gap that impedes financial institutions' efforts to combat financial crimes.

Even conventional frauds weaken the financial system by drawing away government resources geared toward security and by decreasing customer confidence. There needs to be a more mainstream understanding that combating fraud can prevent money laundering and terrorism. As such, a reform to broaden the scope of Section 314 can stay within the terrorism-related goals of the Act while simultaneously protecting the financial system and its customers.

INTRODUCTION

Section 314(b) of the Act permits financial institutions to share information concerning illicit financial transactions amongst themselves. However, because Section 314(b) permits such information sharing only in instances of suspected terrorism and money laundering, banks are constrained in combating other types of financial crime.

In order to best protect the financial system and its customers, the Treasury Department should specify that fraudulent financial transactions fall within the definition of money laundering for the purposes of Section 314(b) or expand the information-sharing safe harbor provided by Section 314(b) to include other types of criminal activity.

THE CHALLENGE

As part of wide-ranging counterterrorism efforts following September 11, 2001, the US Government intensified its focus on illicit financial activity by, or in support of, terrorist organizations. Congress passed the Act to enhance the investigation of terrorist activity, including by strengthening anti-money laundering and anti-terrorist financing provisions. Section 314 of the Act creates stronger links between the banking sector and federal law enforcement and among the financial institutions themselves explicitly to deter money laundering and terrorist financing. These statutory provisions make the financial sector a key factor in the fight against terrorism.

Separated into two sub-parts, both 314(a) and (b) concern the sharing of information as related to individuals, entities, organizations, and countries suspected of possible terrorist financing or money laundering activities. Section 314(a) deals specifically with the financial sector sharing information with law enforcement (usually responding to requests for information and subpoenas) while 314(b) provides the banking sector a safe harbor by authorizing financial institutions and associations of financial institutions to share information amongst themselves.

The limitation with 314(b) lies in the fact that the rule permits financial institutions to share information *only* in instances of suspected terrorism and money laundering. As such, many banks in the United States are unable to share information under the 314(b) safe-harbor program when they suspect customers' funds of being derived from fraudulent activities unrelated to money laundering or terrorism. The fear of liability from sharing information that goes beyond these specific activities potentially hinders full transparency in the Suspicious Activity Reports (SARs) that banks file when they see activities of potential concern.

To alleviate this trepidation, the Financial Crimes Enforcement Center (FinCEN) issued guidance to clarify the scope of information-sharing covered by the safe harbor of Section 314(b).[1] This guidance states that financial institutions, upon following the appropriate statutory notification protocols, may share information with one another about suspected fraud and other "specified unlawful activities"[2] ("SUA") as defined in the federal money laundering statutes (18 USC 1956, 1957). This move by FinCEN to allow information-sharing of suspected SUAs is a step in the right direction, but the banking sector is still constrained by having to link the fraud to money laundering or terrorist activities. For example, if a bank declines a customer for attempting a misrepresentation to obtain a loan, thereby attempting to violate 18 USC 1344(2) ("Bank Fraud"), there is no reason to suspect money laundering or terrorism financing in that transaction. Therefore, because the 314(b) safe harbor does not apply, the bank cannot share information about this customer with other banks in aid of preventing fraud.

[1] See "Guidance on the Scope of Permissible Information Sharing Covered by Section 314(b) Safe Harbor of the USA PATRIOT Act," FinCEN, available at https://www.fincen.gov/sites/default/files/shared/fin-2009-g002.pdf (June 16, 2009).

[2] 18 USC 1956 and 1957 incorporate over ninety offenses as SUAs including mail fraud, wire fraud, bribery, bank fraud, and fraudulent loan and credit applications.

IMPACTS OF LIMITED INFORMATION SHARING

Limiting the exchange of information about fraudulent activity hinders financial institutions from combating a range of crimes that fall outside the definitions of terrorist financing and money laundering. Such an arbitrary restriction directly undermines U.S. national security.

First, and perhaps most significantly, adversaries of the United States take advantage of information silos to fund their illicit activities. In one notable example, hackers believed to be operating on behalf of the North Korean government hacked into the SWIFT global payment messaging system in February 2016 and illicitly transferred $81 million out of accounts held by the Government of Bangladesh at the New York Federal Reserve Bank.[3] Such a brazen theft undermines confidence in SWIFT, in the Federal Reserve Bank of the United States, and in the global financial system writ large. It also likely enriched the government in Pyongyang, thereby bolstering its nuclear weapons program, funding weapons proliferation, and buttressing a regime subject to U.S. and United Nations sanctions.

Limiting the exchange of information about fraudulent activity hinders financial institutions from combating a range of crimes that fall outside the definitions of terrorist financing and money laundering. Such an arbitrary restriction directly undermines U.S. national security.

Due to the absence of ties to money laundering or terrorism, financial institutions would not have been able to share signs of preparation for these transfers. Indicators of such preparations might have included a succession of 35 smaller rapid-fire transfer requests, including 31 that were unsuccessful; information suggesting that the destination accounts had been opened but inactive for almost a year; the failure of Bangladesh Central Bank officials to respond promptly to inquiries about the transfers; an analysis of payment patterns that indicated anomalous behavior; and a comparison of IP addresses, messaging accounts, and destination accounts to those linked to known past frauds.[4] In the wake of the heist, recognizing the imperative to share information that could prevent future illicit transfers, SWIFT CEO Gottfried Liebbrandt called for "drastically improv[ing] information sharing among the global financial community" as part of a five-point plan for addressing cyber crime.[5]

Second, even conventional frauds weaken the financial system by drawing away government resources geared toward security and by decreasing customer confidence, which heightens the industry's vulnerability to money laundering and terrorism. As such, a reform to broaden the scope of Section 314 would be consistent with the purpose of the Act's goal of promoting U.S. national security while still protecting the financial system and its customers.

Third, banks' inability to share their concerns makes it easier for money laundering brokers to use international trade as a means to transfer value of illicit proceeds. As an example, brokers employ couriers to structure cash deposits into U.S. bank accounts in amounts less than $10,000 to avoid triggering currency transaction report (CTR) filings. The funds are then transferred to U.S.-based businesses either via wire or bank draft to pay for legitimate foreign trade involving the export of U.S. goods. The criminal organizations sell their U.S. dollars at a discount to these brokers for local currency, and foreign importers buy the U.S. dollars to pay for their imported goods or forward proceeds electronically to a front company. According to law enforcement officials at the multi-agency El Dorado Money Laundering Task Force in New York, this activity continues to be the preferred method to introduce illicit cash into the U.S. financial system.

[3] Michael Corkery and Matthew Goldstein, "North Korea Said to be Target of Inquiry Over $81 Million Cyberheist," New York Times, March 22, 2017. At https://www.nytimes.com/2017/03/22/business/dealbook/north-korea-said-to-be-target-of-inquiry-over-81-million-cyberheist.html?_r=0.

[4] Kim Zetter, "That Insane, $81m Bangladesh Bank Heist? Here's What We Know," Wired, May 17, 2016. At https://www.wired.com/2016/05/insane-81m-bangladesh-bank-heist-heres-know/. Also Andrew MacAskill and Jim Finkle, "U.K. banks ordered to review cyber security after SWIFT heist," Thomson Reuters, May 18, 2016. At https://www.reuters.com/article/us-cyber-heist-bankofengland/exclusive-uk-banks-ordered-to-review-cyber-security-after-swift-heist-idUSKCN0Y92KR. Also SWIFT CEO Gottfried Liebbrandt, speech to 14th annual European Financial Services Conference, Brussels, May 24, 2016. At https://www.swift.com/insights/press-releases/gottfried-leibbrandt-on-cyber-security-and-innovation. Also John Wetzel, "Neighborhood Watch: Identifying Early Indicators of the Central Bank of Bangladesh Heist," March 29, 2016. At https://www.recordedfuture.com/bangladesh-bank-heist/.

[5] SWIFT CEO Gottfried Liebbrandt, speech to 14th annual European Financial Services Conference, Brussels, May 24, 2016. At https://www.swift.com/insights/press-releases/gottfried-leibbrandt-on-cyber-security-and-innovation.

> The lack of an information-sharing mechanism among financial institutions regarding the closing and opening of accounts leaves the U.S. financial system at risk.

Banks eventually detect the activity within an account, file one or more SARs, and exit the customer from the bank. Upon being exited, the customer either wires his balance or writes a check to another U.S. financial institution, and the pattern repeats itself. In effect, brokers can use accounts disposably, like burner phones, to continue their activity unabated. U.S. financial institutions are often aware of where their exited customers have moved their banking operations. As a result, the ability to warn other banks of potentially fraudulent activities could prevent the customer from opening a new bank account and depositing the transferred funds into the U.S. banking system. Converting cash into electronic funds is the first step in transferring the value of that cash to criminal and terrorist organizations and integrating it into the economy. The lack of an information-sharing mechanism among financial institutions regarding the closing and opening of accounts leaves the U.S. financial system at risk.

Financial institutions are sensitive to this restriction, but what hinders the industry in the fight against financial crimes—more than the nominal constraints in the law—is financial institutions' aversion to risk. As inherently cautious institutions, banks often fail to discuss and share customer information even when permitted to do so unless they are provided definitive guidance from the government.

RECOMMENDATIONS

1. In order to best protect the financial system and its customers, FinCEN should either (1) provide guidance that financial transactions, which support a fraud and the transfer of proceeds of a fraud, fall within the definition of money laundering for 314(b) purposes, or (2) expand its 314(b) information-sharing safe harbor to include all instances of possible fraud and any potential criminal activity.

2. The current standard requiring that information shared pursuant to 314(b) must relate to potential money laundering or terrorist financing and related SUAs is limited given the current risks facing financial institutions from traditional non-SUA fraud as well as emerging cyber related fraud threats and malware. The financial industry would benefit from additional guidance from FinCEN to address 21st Century risks.

3. FinCEN should consider using its information sharing capability to conduct targeted outreach with the financial industry, especially smaller regional banks and credit unions that do not have sophisticated AML compliance programs or institutional knowledge of money laundering, and FinCEN should hold open discussions on categories of threats and other signs about which financial institutions should be aware.

4. Given that criminals often change their tactics in the wake of law enforcement actions, FinCEN should team with law enforcement agencies to inform the financial community of new patterns of criminal behavior as soon as they are detected.

5. With revised FINCEN guidance and/or clear safe harbor protections, a number of private sector entities could also facilitate the sharing of information between financial institutions. The Financial Services Information Sharing and Analysis Center (FS-ISAC) facilitates the timely sharing of both physical and cyber threat information across the financial services industry and with federal, state and local government agencies. Similarly, the National Cyber-Forensics and Training Alliance (NCFTA) develops and shares intelligence to prevent and mitigate cyber threats to the financial services industry. Should changes to the regulatory environment permit greater information sharing on fraudulent financial activities, FS-ISAC and NCFTA should develop mechanisms for using their existing procedures and infrastructure to disseminate such data and integrate it with their existing streams of threat information.

6. INSA's Financial Threats Council endorses a report published in February 2017, titled: *A New Paradigm: Redesigning the U.S. AML/CFT Framework to Protect National Security and Aid Law Enforcement.*[6] This report was the work of a group of approximately 60 anti-money laundering (AML) experts who addressed the incentives the industry has (or lacks) to innovate and identify criminal behavior. Their recommendations call for an expansion of the protections granted to financial institutions for sharing information and incentivizing innovative protocols in crime detection.

[6] The Clearing House, A New Paradigm: Redesigning the U.S. AML/CFT Framework to Protect National Security and Aid Law Enforcement, February 2017. At :https://www.theclearinghouse.org/~/media/TCH/Documents/TCH%20WEEKLY/2017/20170216_TCH_Report_AML_CFT_Framework_Redesign.pdf.

ABOUT INSA

The Intelligence and National Security Alliance (INSA) is a nonpartisan, nonprofit forum for advancing intelligence and national security priorities through public-private partnerships. INSA works to make government more effective and efficient through the application of industry expertise and commercial best practices. INSA's 160+ member organizations are leaders in intelligence collection and analysis, data analytics, management consulting, technology development, cybersecurity, homeland security, and national security law, and its 4,000 individual members include leaders, senior executives, and intelligence experts in government, industry, and academia.

ABOUT THE INSA FINANCIAL THREATS COUNCIL

INSA's Financial Threats Council works to provide a deeper understanding of the broad range of financial threats to U.S. national security; strengthen public-private cooperation and information sharing regarding financial vulnerabilities; and establish tools and processes to counter efforts to exploit such vulnerabilities.

ACKNOWLEDGEMENTS

INSA appreciates the efforts of members and staff who contributed to the development of this paper.

Financial Threats Council

Sonny Carpenter
Baker Hostetler

Kevin Delli-Colli
Deloitte

John Suver
Bank of America

James Katavalos, Council Chair
Citigroup

Leslie Ireland, Council Vice Chair

INSA Leadership and Staff

Chuck Alsup, *President*

Suzanne Wilson-Houck, *Chief Operating Officer*

Larry Hanauer, *Vice President for Policy*

Ryan Pretzer, *Senior Manager, Policy and Public Relations*

Amy Cooper, *Intern*

Eric Bigelow, *Intern*

Alexzandra Smith, *Intern*

INTELLIGENCE AND NATIONAL SECURITY ALLIANCE

Building a Stronger Intelligence Community

(703) 224-4672 | www.INSAonline.org