UNITED STATES DEPARTMENT OF THE TREASURY

FinCEN

FINANCIAL CRIMES ENFORCEMENT NETWORK

JENNIFER SHASKY CALVERY
DIRECTOR
FINANCIAL CRIMES ENFORCEMENT NETWORK

FSSCC-FBIIC JOINT MEETING
NEW YORK, NY
DECEMBER 9, 2015

Good afternoon. It is a pleasure to be joining you for the FSSCC-FBIIC joint meeting.

I would like to begin today by giving a brief overview of FinCEN and the specialized work we do in the area of financial intelligence. This will set the stage for a discussion of how we are harnessing both technology and data to combat some of our nation's greatest threats, including cyber threats, which I know is of particular interest for our discussion today.

The Financial Crimes Enforcement Network, known as "FinCEN," is a part of the Treasury Department. We serve in two roles. First, we are the Financial Intelligence Unit (FIU) for the United States. This is a term of art. Most countries around the world have an FIU that is responsible for collecting, analyzing, and disseminating financial intelligence to law enforcement and other relevant authorities to help fight money laundering and the financing of terrorism. Secondly, we are the lead anti-money laundering/countering the financing of terrorism (AML/CFT) regulator for the federal government.

As the nation's FIU and AML/CFT regulator, FinCEN is uniquely positioned to collect cyber threat information, to exploit it, and share it with U.S. government partners as well as external stakeholders. And in both roles, our mission is to safeguard the financial system, combat money laundering, and promote national security.

The FinCEN Data and Technology Footprint

So, where does FinCEN get its data or so-called "financial intelligence?" The Bank Secrecy Act (BSA) is a set of provisions constituting our AML laws in the United States. The BSA requires a broad range of U.S. financial institutions to maintain records and provide reporting to FinCEN. The majority of the BSA data FinCEN collects comes from two reporting streams: one on large cash transactions exceeding $10,000, and the other on suspicious transactions identified by financial institutions.

So when financial institutions provide reporting to FinCEN, they do so pursuant to the BSA so we call the reporting stream "BSA reporting" or "BSA data." And the term "financial institution" is quite broad. It includes:

- Banks and credit unions
- Money remitters, check cashers, and virtual currency exchangers
- Dealers in foreign exchange
- Casinos and card clubs
- Insurance companies
- Securities and futures brokers
- Mutual funds
- Operators of credit card systems
- Dealers in precious metals, stones, or jewels
- Certain individuals and trades or businesses, transporting or accepting large amounts of cash

I know this is a long list, but I think it illustrates the rich and diverse sources of data we have at our disposal to help safeguard the integrity of our financial system and combat a wide range of criminal and national security threats.

We also collect information on cash crossing the U.S. border, for example when you arrive and depart the country. We require reports from any retail store when it receives large cash payments. We collect reports for individuals with foreign bank accounts. And we collect all kinds of specialized and targeted data. Taken together, BSA data includes nearly 190 million records.

On average, we receive approximately 55,000 electronically filed BSA reports from more than 80,000 financial institutions and 500,000 individual foreign bank account holders each day through an IT system we developed known as E-filing. We then make this information available to more than 9,000 law enforcement and regulator users through a search tool we designed to meet their specialized needs, known as FinCEN Query. They, in turn, make approximately 30,000 searches of the data each day. E-filing not only streamlines reporting for tens of thousands of financial institutions and hundreds of thousands of individual filers, it also helps the users of the BSA data by making BSA reports searchable in FinCEN Query in two days, rather than a minimum of two weeks if filed on paper.

FinCEN's recent analytical enhancements have enabled our analysts to provide critical tactical and strategic insight to our law enforcement, intelligence community, and international partners. By applying cutting edge tools and automated search capabilities to the data, the analytical products we produce are now more timely and valuable.

FinCEN has also fostered strong partnerships with other public sector organizations to enhance our advanced analytical capabilities. For instance, FinCEN works closely with the

Defense Advanced Research Projects Agency (DARPA) to leverage its deep expertise in large scale data analysis and visualization, further assisting FinCEN to fully exploit the BSA data.

FinCEN is also working with DARPA to apply a number of open source tools to the BSA data. These tools provide FinCEN analysts with the capability to visually analyze filing patterns by states, regions, and countries; explore and analyze networks of activity within and across BSA filings; and trace transactional activity and financial flows between entities.

Our IT efforts reach globally as well. As the FIU for the United States, FinCEN interacts with 150 other foreign FIUs and provides the application allowing FIUs to securely interact and exchange information with each other. In the last several months, FinCEN has used this secure environment to help our FIU partners coordinate across multiple jurisdictions to freeze millions of dollars in assets obtained by malicious cyber actors as they attempted to move the funds internationally.

The Value of SARs in Combatting Cyber Threats

The purpose and attribution for a cyber-attack are rarely clear at the time the attack occurs, and malicious cyber actors will often test their hacking tools on entities such as banks before they deploy them elsewhere. FinCEN receives early reporting from financial institutions on cyber activity that is suspicious before it ripens into a full cyber incident.

These Suspicious Activity Reports, known as "SARs" often contain information that could be helpful in deflecting cyber-attacks and identifying their source. This information includes attribution factors, such as IP addresses, timestamps, e-mail addresses, and the nature of the suspicious activity. It may also include information relevant to the target of the attack which can be compared against other information to detect patterns of interest by malicious cyber actors.

In addition to helping identify the source of cyber-attacks, the attribution information included in SARs allows FinCEN to follow the money and identify the malicious cyber actors or networks receiving payment for conducting illicit financial activities. It also allows FinCEN to identify members of any money laundering network helping to move and hide the money. Finally, FinCEN uses this information to map the trail of funds which is crucial to recovering funds maliciously obtained by cyber actors.

Information about suspicious cyber activity involving the financial sector is of interest to many different law enforcement agencies depending on the nature of the activity and the victim. FinCEN shares cyber threat information and our analysis with U.S. law enforcement agencies, regulators, and foreign partners, when appropriate. FinCEN also grants over 300 federal, state, and local law enforcement and regulatory agencies in the United States direct access to the data through FinCEN Query. And as I mentioned earlier, they, in turn make

approximately 30,000 queries of the data each day to pursue investigations on a variety of topics.

The FinCEN Intelligence Cycle

FinCEN delivers financial intelligence to law enforcement, regulatory, foreign, and private sector partners following an intelligence cycle methodology. In using the word "intelligence" I should clarify that FinCEN is not a part of the intelligence community. However, anyone who deals with this amount of data goes through some form of business intelligence cycle. And for FinCEN, our intelligence cycle involves the collection, processing, exploitation, dissemination, and direction of future collection efforts. In this respect, FinCEN is unique in that we have autonomous control over all elements of our intelligence cycle.

In terms of collection, the first stage of the intelligence cycle, FinCEN has the ability to collect more than routinely filed BSA reporting. We also have the ability to proactively target certain financial intelligence for collection using a variety of authorities and special measures. Some of these targeted financial intelligence collections include:

- Section 311, which is a provision of the USA PATRIOT Act that enables FinCEN to require U.S. financial institutions to collect targeted financial intelligence on: (i) a foreign jurisdiction, (ii) a foreign financial institution, (iii) a class of transactions, or (iv) a type of account, if the Director of FinCEN finds it is of "primary money laundering concern."

- Section 314(a), which is a provision of the USA PATRIOT Act that enables FinCEN to share law enforcement and regulatory information with financial institutions on individuals, entities, and organizations reasonably suspected of engaging in terrorist acts or money laundering activities, in order to collect related financial intelligence.

- A Geographic Targeting Order (GTO), which is issued by FinCEN to impose additional recordkeeping or reporting requirements on domestic financial institutions or other businesses in a specific geographic area identified in the order.

Processing is the second stage of the intelligence cycle. With approximately 55,000 discrete filings per day, advanced technology solutions are needed to review and quickly disseminate time-sensitive information. In order to manage a data collection of this size and rapidly identify nodes and patterns of potentially illicit activity for further action, FinCEN employs a number of advanced analytic approaches.

In order to identify cyber-related information in its vast data pool, FinCEN employs business rules to screen filings on a daily basis. These rules generate alerts which help FinCEN produce timely strategic and tactical analytic reports on cyber-related threats for U.S. government stakeholders including law enforcement, regulators, the intelligence community, and foreign partners, as appropriate and legally permissible. While other agencies have access

to FinCEN's database, FinCEN's business rules allow it to identify information that may not be obvious to agencies querying our database. FinCEN may take fairly undeveloped SAR information, compare it against other BSA data and open source material that may provide context, and develop a meaningful, well-founded lead or piece of intelligence that can assist U.S. government partners as well as external stakeholders.

In the analysis and dissemination stages of our intelligence cycle, FinCEN has consolidated analytic capabilities and expanded the scope of our work to create products that address critical priority threats for our stakeholders. We combine BSA data with additional intelligence information, commercial data sources, and other open source material, as experts in financial intelligence. The focus of FinCEN's analytic work has shifted to more proactive targets and strategic assessments of money laundering trends and vulnerabilities.

In addition to expanding our analytic scope, FinCEN continues to develop unparalleled expertise in money laundering methodologies, emergent financial sectors, such as virtual currencies, and cyber threats. And our analysts actively provide substantive training to other U.S. government agencies on these issues.

Lastly, the intelligence cycle helps inform our future planning and direction. We use our regulatory rulemaking authority to, among other things, define the reporting financial institutions and others must provide to FinCEN. We then use our Financial Institution Advisory Program to help industry understand the telltale signs of the suspicious activity that is worthy of reporting. FinCEN issues both public and non-public advisories to alert financial institutions of specific illicit finance risks such as cyber threats, including the red flag indicators in their data that might be indicative of suspicious activity and helpful to law enforcement. FinCEN's cyber-related Advisories have provided financial institutions with guidance to help them guard against cyber threats emanating from the darknet, as well as information on the transition of Internet Protocol addresses from version 4 to version 6.

Our rulemaking activities and advisories expand and/or improve the information that FinCEN collects. The dovetailing of this phase with the collection phase confirms the iterative and cyclical nature of our intelligence activities.

Examples of FinCEN Partnership, Data, and Analytics in Action

Central to FinCEN's responsibilities is the statutory mandate to bring together partners from law enforcement, the private sector, government, and international counterparts to identify and combat threats to the financial system. FinCEN chairs the Bank Secrecy Advisory Group, which brings our law enforcement, regulatory, and financial industry partners together multiple times a year to discuss issues relevant to combating terrorist financing and money laundering, including cyber threats. FinCEN has also been one of the most actively engaged agencies in the U.S. government in conducting cybersecurity outreach: providing training, issuing guidance, disseminating intelligence, and contributing to the U.S. government's cybersecurity strategy.

FinCEN is also working with its international and law enforcement partners to combat global cyber threats. In recent years, law enforcement has seen an increase in spear phishing cases against middle to high-value business targets. These are instances where cyber criminals obtain and replicate an enterprises' wire transfer information and send the authenticated data to the compromised company's financial institution. The financial institution then wires the funds to an overseas bank account that the criminals control.

The Federal Bureau of Investigation (FBI) has documented over $1 billion in losses globally through this criminal scheme since they began tabulating the figures in 2013. FinCEN has partnered with the FBI and the United States Secret Service (USSS), to rapidly identify and recover assets stolen from businesses under various business email compromise schemes.

FinCEN leverages its relationships with counterpart FIUs to encourage foreign authorities to intercede and freeze funds or reverse wire transfers. FinCEN's Global Rapid Response Program, which began in October 2014, has completed over 160 requests to foreign FIUs on behalf of the FBI, USSS, and various U.S. financial institutions. The multi-tiered partnership between law enforcement, FIUs, and financial institutions has helped to secure the recovery of more than $137 million.

I spoke earlier about the BSA data we collect, and this information is proving to be very valuable as we work to confront cyber threats.

FinCEN is actively analyzing BSA data to analyze and develop leads on cyber threats including ransomware, DDOS attacks, and malware targeting financial institutions. FinCEN also provides our law enforcement stakeholders with tactical and strategic intelligence reports associated with these threats. Through our efforts, FinCEN builds on its partnerships with the private sector and law enforcement agencies to deter and detect illicit cyber activity by receiving, analyzing, and sharing financial intelligence.

For example, SARs filed by several different financial institutions played a vital role in furthering an investigation where a regional Florida bank had nearly $7 million fraudulently wired out of one of its accounts. An FBI investigation confirmed that a computer at the Florida bank was infected with the GameOver Zeus virus, and that the infected computer was used to steal the credentials that were used to initiate the fraudulent transfer.

The SARs that were filed helped the FBI identify several wire transfers related to one co-conspirator involved in a large scale money laundering organization acting on behalf of GameOver Zeus, which, in turn, led to further significant investigative gains. The total losses associated with this GameOver Zeus botnet are believed to exceed $100 million in the United States alone. The group responsible is based in Russia and Ukraine, and deliberately targeted their malicious software at U.S. individuals and companies.

The Importance of Information Sharing

A key component to guarding against cyber threats is information sharing within the institution itself. If I could leave each of you with one piece of advice, which I have been discussing since FinCEN issued its "Culture of Compliance" Advisory in August 2014, it would be to share information across the business lines of your institution. As noted in the Advisory, there is information in various departments within a financial institution that may be useful and should be shared. For example, information developed by those in your institution that work to combat cyber threats could also assist your institution in complying with its BSA/AML obligations and assisting law enforcement to combat those threats. So my hope would be that after you leave here today, you will seek out your institution's AML officer to discuss how you can share information with each other that will ultimately benefit your entire institution through enhanced information sharing with law enforcement.

FinCEN also is strongly encouraging financial institutions to leverage their internal information technology resources to include cyber-derived information (such as IP addresses or bitcoin wallet addresses) in suspicious activity reports; to file these SARs voluntarily on cyber-attacks, and, to participate in voluntary information sharing with other financial institutions under the safe harbor granted in Section 314(b) of the USA PATRIOT Act.

I would like to underscore this point regarding IP address information: Less than two percent of SARs filed contain IP information. This information is incredibly important to the FinCEN analysts and law enforcement investigators working to combat cyber-crimes.

Information sharing between FinCEN and the financial industry is critically important as well. While FinCEN is constrained from sharing certain SAR information with financial institutions, such as the filing institution or the customer and account information, we can provide "research, analytical and informational services to financial institutions … to assist … in the detection and prevention of terrorism, organized crime, money laundering, and other financial crimes." This allows FinCEN to share attribution information derived from SARs and subjected to analysis that does not otherwise reveal sensitive customer or filer information. We are currently in the process of exploring ways to share cyber threat information derived from BSA reports with U.S. financial institutions in efforts to prevent and guard against cyber-attacks and cyber-enabled crime and protect the critical infrastructure.

FinCEN also works closely with Treasury components to develop strategies that combat threats and protect the integrity of the financial system. FinCEN has worked with the Office of Domestic Finance's Financial Sector Cyber Intelligence Group on disseminating its intelligence products to raise awareness on cyber-enabled threats. FinCEN also works closely with the Office of Terrorist Financing and Financial Crimes to gather information from financial institutions about the financial institutions' cybersecurity strengths and weaknesses.

Conclusion

I hope in my time today I have provided you with a sense of how FinCEN is working to address cyber threats to our financial system. It is clear to me that the FBIIC and FSSCC recognize the importance of sharing timely and actionable information to combat these threats, and this is the key to our efforts at FinCEN as well. We are fortunate to have a variety of tools at our disposal to make a real impact against these significant threats, but the most effective tool we have is partnerships with our law enforcement, regulatory, and financial industry partners through forums such as this one today.

###