UNITED STATES DEPARTMENT OF THE TREASURY

FinCEN

FINANCIAL CRIMES ENFORCEMENT NETWORK

JENNIFER SHASKY CALVERY
DIRECTOR
FINANCIAL CRIMES ENFORCEMENT NETWORK

PREDICTIVE ANALYTICS WORLD FOR GOVERNMENT
WASHINGTON, DC
OCTOBER 13, 2015

Good afternoon. It is a pleasure to be joining you for the Predictive Analytics World for Government conference.

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 terrorist organizations, foreign corruption, cyber threats, transnational criminal and drug trafficking organizations, and massive fraud schemes.

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 a financial intelligence unit and in each, the FIU 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. 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 anti-money laundering 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. 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; and
- 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.

To ensure that the BSA data gets into the right hands in a timely fashion requires state of the art technology. When I first arrived at FinCEN three years ago, I assumed FinCEN's IT department was similar to one you might find in any government agency or private sector business that manages the organization's day-to-day IT environment. What I quickly learned is it is anything but. FinCEN's IT team not only manages our internal IT environment, but is also responsible for much more. They had also begun laying the foundation to become an IT and data science leader in government.

Just as I became Director, FinCEN was wrapping up a 5-year program to modernize the process of collecting, analyzing, and disseminating the BSA data. I am very proud to say that the program continuously and successfully delivered on time and within budget on milestones established by the Office of Management and Budget. Even more, of the six Treasury Inspector General Reports delivered throughout the process, the last three resulted in "No Recommendations." I am sure you will agree this is an incredible accomplishment in the Government IT world, and a true testament to those FinCEN employees involved in this effort.

Through the modernization program, we accomplished four significant goals: (1) we assumed responsibility for maintaining our own data in a FinCEN system of record; (2) we supported a significant shift from the paper filing of BSA reports to the electronic filing of BSA data; (3) we developed a new IT system for our many law enforcement and regulatory partners to

search, slice, and dice BSA data; and (4) we provided advanced analytics tools to FinCEN's analysts to enhance their capabilities to make sense of the data.

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 their 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 multi-national jurisdictions to freeze millions of dollars in assets of illicit actors trying to move funds internationally.

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 it has autonomous control over all elements of its intelligence cycle.

In terms of collection, the first stage of the intelligence cycle, FinCEN has the ability to collect more than routinely filed BSA data. 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.

To combat our most significant money laundering and terrorist financing threats, FinCEN employs more than one hundred automated business rules to screen filings on a daily basis and identifies reports that merit further review by analysts. The rules range in complexity from traditional "watchlist" rules designed to identify known illicit actors to complex multi-variable weighted rule sets capable of identifying potential illicit activity.

FinCEN's rules program generates more than 250 findings per day, providing an important stream of timely intelligence to our analysts and external stakeholders. Our data scientists and analysts work together, often with input from investigators internal and external to FinCEN, to design models and analytic techniques that identify newly trending illicit typologies; monitor responses to our advisories, geographic targeting orders, and other activities; locate potential data quality issues; and flag subjects not currently under investigation who exhibit behavior patterns indicative of significant money laundering activity.

FinCEN has also begun leveraging advanced statistical methodologies to benchmark BSA filing volumes by financial sector. These sector benchmarking studies have provided FinCEN with a greater awareness of the filing patterns of institutions within specific industry

sectors and have helped us quickly identify institutions which may have deficient anti-money laundering controls, or in some extreme cases, may actually be facilitating illicit activity.

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, including the financial industry. 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. Once we identify threats and vulnerabilities, FinCEN adjusts the regulatory framework protecting the U.S. financial system. We use our regulatory rulemaking authority to, among other things, define the reporting financial institutions and others must provide to FinCEN. We also develop advisories to inform industry about money laundering and terrorist financing threats, including the red flag indicators in their data that might be indicative of suspicious activity. 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 Data, Technology, and Analytics in Action

Let me turn now to some examples of FinCEN data, technology, and analytics in action. Today, there is perhaps no greater threat than the one posed by al-Qa'ida, the Islamic State in Iraq and the Levant (ISIL), their respective affiliates, and in particular by foreign terrorist fighters, i.e., those individuals seeking to go to conflict areas in Syria, Iraq, and elsewhere to fight for terrorist groups. The reporting financial institutions provide has already proven to be an essential component in identifying foreign terrorist fighters, their financial facilitators, and the flow of funds.

I mentioned our rules program earlier, but I would like to spend a few minutes discussing our analysis in action. Thanks to the reports filed by financial institutions, FinCEN has a wealth of data that we are able to analyze and disseminate in the form of financial intelligence to our Treasury colleagues, and to law enforcement and intelligence community partners. For example, the ISIL related business rules alone generate more than 1,000 matches each month for further review and exploitation; these matches are reviewed by analysts on a daily basis. BSA data that triggers rule hits is summarized and disseminated as Flash reports or, with additional analytic

content to law enforcement partners, regulatory agencies, the intelligence community, and relevant foreign partners. These Flash reports allow the FBI to identify, track, and disrupt the activities of potential foreign terrorist fighters and support U.S. Customs and Border Patrol (CBP) efforts to prevent foreign terrorist fighters from leaving or entering the United States.

FinCEN's analytics program is also proving to be an effective tool in combatting fraud. While supporting ongoing law enforcement efforts to combat healthcare fraud against the United States government, FinCEN discovered that compromised check cashers were facilitating the fraud. Using behavior patterns of known compromised check cashers, FinCEN created a multi-variable weighted rule set designed to identify check cashers involved in similar activity in other jurisdictions. This project was used to support investigative efforts by the U.S. Attorney's office for the Southern District of New York as well as multiple jurisdictions and agencies in Florida.

Let me provide you with a few concrete examples of how we further shape the collection of BSA data by using FinCEN's tools and authorities. FinCEN issues both public and non-public advisories to financial institutions concerning money laundering or terrorist financing threats and vulnerabilities for the purpose of enabling financial institutions to guard against such threats. Advisories contain guidance on complying with our regulations to address those threats and vulnerabilities.

In May 2015, FinCEN issued a non-public Advisory related to ISIL financing. Within less than a week of its publication, this Advisory was read by financial institutions more than 34,000 times (for context, the normal statistic is about 3,000 hits per month for a non-public Advisory). As of September, that number had grown to over 73,000. More importantly, through FinCEN's financial institution hotline, which allows financial institutions to reach out to FinCEN 24/7 to report possible terrorist financing activity, we were alerted that numerous reports of suspicious activity were filed on the basis of this Advisory. This included reporting on suspicious activity previously filed where the reporter had not realized at the time it was ISIL-related, as well as new reporting of suspicious activity specifically referencing the Advisory. It is important to note that both large and small financial institutions made reports, which demonstrates the utility of our collection process and the seriousness the financial industry attaches to its data reporting obligations.

In another example, our review of suspicious activity reports filed by U.S. financial institutions, together with information from law enforcement, showed us that Mexico-based criminal organizations were continuing to employ funnel accounts to move illicit proceeds. A funnel account is when an individual or business account in one geographic area receives multiple cash deposits, often in amounts below the cash reporting threshold, and from which the funds are withdrawn in a different geographic area with little time elapsing between the deposits and withdrawals. It was also clear from our analysis that funnel accounts are being used to finance the purchase of goods as part of trade-based money laundering (TBML) activity.

This analysis led FinCEN to issue a public Advisory in May 2014 to alert financial institutions of the increased use of funnel accounts to move illicit proceeds and to finance TBML. The Advisory provided red-flags to assist financial institutions to identify and report suspicious activity possibly tied to criminal organizations. And in September 2014, FinCEN issued a GTO aimed at curbing TBML. The GTO imposed certain reporting and recordkeeping requirements on several covered businesses in the City of Los Angeles, California.

After the Advisory was issued, there was a significant increase in the number of suspicious activity reports filed by financial institutions. In the 2012-2013 timeframe, prior to the 2014 Advisory, there were 123 suspicious activity reports filed referencing funnel account activity. However, during 2014 there were nearly 10,000 such filings. This 8,000% increase in funnel account and TBML filings drastically improved our collection efforts; and thanks to E-filing, allowed us to immediately get these reports into the hands of thousands of law enforcement users through FinCEN Query.

Conclusion

As I conclude today, I would like to note that FinCEN's technology focus extends beyond our analytical efforts. Even on the regulatory side, as the administrator of the BSA, FinCEN is finding itself on the front-lines of emerging technologies. FinCEN has been one of the most active government leaders in the virtual currency area, issuing guidance over two and a half years ago clarifying regulatory requirements.

As an employer of IT professionals and data scientists, we face the same challenges as many organizations to compete for the very best talent in an ever-changing technology world. We are fortunate at FinCEN to have some of the very best minds helping us keep pace with these changes. And we are always looking for great people to add to our team. Please visit our website at www.fincen.gov and click on the "Careers" tab to learn about employment opportunities.

Even on the workforce performance front, we are using the latest in data analytics to improve employee engagement at FinCEN. We recently partnered with a leading global consulting company to gather information and help us develop action plans so all FinCEN employees are actively engaged in our mission and in the organization.

I hope in my time today I have provided you with a sense of how technology and data impact all that we do. I hope I also provided some insight into how FinCEN is working to harness advanced analytics to address threats to our financial system. We are fortunate to have a variety of analytical tools at our disposal to make a real impact against these unprecedented and significant threats, but the most effective tool we have is our people and our many partners throughout government and the private sector.

###