UNITED STATES DEPARTMENT OF THE TREASURY

FinCEN

FINANCIAL CRIMES ENFORCEMENT NETWORK

STATEMENT OF

JAMAL EL-HINDI, ACTING DIRECTOR
FINANCIAL CRIMES ENFORCEMENT NETWORK
UNITED STATES DEPARTMENT OF THE TREASURY

BEFORE THE

UNITED STATES HOUSE OF REPRESENTATIVES
COMMITTEE ON FINANCIAL SERVICES
SUBCOMMITTEE ON TERRORISM AND ILLICIT FINANCE

APRIL 27, 2017

NOT FOR PUBLICATION UNTIL RELEASED BY THE HOUSE COMMITTEE ON FINANCIAL SERVICES, SUBCOMMITTEE ON TERRORISM AND ILLICIT FINANCE

Chairman Pearce, Vice Chairman Pittenger, Ranking Member Perlmutter, and distinguished members of the Subcommittee, thank you for inviting me to appear before you today to discuss the role of the Financial Crimes Enforcement Network (FinCEN) in collecting, analyzing, and disseminating Bank Secrecy Act (BSA) data, and to share with you some new and evolving money laundering and terrorist financing challenges. I appreciate the Subcommittee's interest in these important issues and your continued support of our efforts.

FinCEN – a bureau of the U.S. Department of the Treasury within the Office of Terrorism and Financial Intelligence (TFI) – is charged with safeguarding the financial system from illicit use, combating money laundering, and promoting national security through the collection, analysis, and dissemination of BSA information and strategic use of BSA authorities. We strive for the responsible use of financial information for greater security and integrity of the U.S. financial system. FinCEN works to achieve its mission through a broad range of interrelated strategies, including:

- Implementing, administering, and enforcing the BSA – the United States' primary anti-money laundering and countering the financing of terrorism (AML/CFT) regulatory regime;
- Supporting law enforcement, intelligence and regulatory agencies through the sharing and analysis of BSA information;
- Serving as the Financial Intelligence Unit (FIU) for the United States; and
- Building international cooperation and technical expertise among the global network of FIUs.

To accomplish these activities, FinCEN employs a team of dedicated employees with a broad range of expertise in illicit finance, financial intelligence, the financial industry, the AML/CFT regulatory regime, technology, and enforcement. FinCEN's ability to work closely with regulatory, law enforcement, international, and industry partners promotes consistency across our regulatory regime and protects the U.S. financial system.

Collection, Analysis and Dissemination of Bank Secrecy Act Data

The BSA is the primary federal AML law. It requires a broad range of U.S. financial institutions to establish AML programs, maintain records, and provide reports to FinCEN. The majority of BSA data FinCEN collects comes from two reporting streams: Currency Transaction Reports (CTRs) and Suspicious Activity Reports (SARs). Financial institutions[1] must file CTRs with FinCEN for cash transactions totaling more than $10,000 and file SARs to report suspicious transactions. Both the objective reporting in CTRs and the subjective reporting in SARs are critically important; they provide a wealth of potentially useful information to FinCEN and other agencies working to detect and prevent money laundering, other financial crimes, and terrorism.

Thanks to funding from Congress, FinCEN successfully completed an Information Technology (IT) modernization program in 2014, updating the process of collecting, analyzing and disseminating BSA data. FinCEN accomplished five significant goals through this program: FinCEN 1) assumed responsibility for maintaining BSA data in a FinCEN-based system; 2) shifted from paper filings of BSA reports to the electronic filing of BSA reports; 3) developed a new IT system for approved law enforcement and regulatory partners to access BSA data; 4) strengthened IT security through implementation of two-factor authentication and other mechanisms; and 5) developed foundational advanced analytics capabilities to enhance FinCEN's ability to exploit BSA data.

FinCEN receives an average of roughly 55,000 new financial institution filings each day. These filings come from more than 80,000 financial institutions and 500,000 individual foreign bank account holders through FinCEN's modernized E-filing system. FinCEN maintains over 200 million of these BSA filings in our database. FinCEN makes this information available to more than 10,000 law enforcement and other government users through a search tool designed to meet their specialized needs, known as FinCEN Query. These users, in turn, perform approximately 30,000 daily searches of the data. E-filing has streamlined the reporting process for financial institutions and individual filers and significantly improved users' ability to exploit BSA data by making it more accessible and searchable.

---

[1] Examples of institutions that file SARs and/or CTRs include: banks and credit unions, money remitters, check cashers, virtual currency exchangers, casinos and card clubs, and dealers in foreign exchange.

The protection of the sensitive information we receive is also a critical part of our mission. FinCEN safeguards BSA data through a continual process of reviewing IT security measures and processes in place, adjusting to current and emerging risks, and ensuring that security is a consistent requirement considered throughout the lifecycle of each system. FinCEN systems are accredited to High Federal Information Security Management Act (FISMA) levels and employ strong security mechanisms such as two-factor authentication, encryption, and activity monitoring to protect BSA data. FinCEN works with the Department of the Treasury and the Department of Homeland Security cyber security organizations for security operations and mitigation activities.

The FinCEN Financial Intelligence Cycle

FinCEN delivers BSA information and related analysis to law enforcement, regulatory, foreign, and private sector partners following an intelligence cycle methodology. This cycle involves the collection, processing, exploitation, and dissemination of BSA-derived financial intelligence, and the direction of future BSA collection efforts

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

- Section 314(a) of the USA PATRIOT Act, which authorizes 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.

- Geographic Targeting Order (GTO) authority, which enables FinCEN to impose additional recordkeeping or reporting requirements on domestic financial institutions or other businesses in a specific geographic area identified in the order for 180 days.

- Foreign Financial Agency authority, which enables FinCEN to impose additional reporting requirements on U.S. financial institutions about their transactions with designated foreign financial entities.

- Demand Letters, which are requests by FinCEN for records relating to international funds transfers of $3,000 or more. The scope of the requested information can vary depending on the specific circumstances of the request.

Processing is the second stage of the financial intelligence cycle. With approximately 55,000 filings per day, advanced technology solutions are needed to review, analyze, and quickly disseminate time-sensitive information. To manage a data collection of this size and to 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 automated business rules to screen filings on a daily basis and identify reports that merit further review by analysts. The rules range in complexity from traditional "watch list" rules designed to identify known illicit actors to complex multi-variable weighted rule sets capable of identifying potential illicit activity.

These algorithms search the reporting for key terms, entities, and typologies of interest daily, across six priority areas: transnational security threats; cybercrime; transnational organized crime; significant fraud; compromised financial institutions or third party money laundering; and data quality, benchmarking, and anomaly detection. The business rules produce approximately 5,000 rule findings per month, pointing FinCEN analysts to specific filings for hands-on review and focusing their efforts on the filings most likely to be key to defending against priority threats. This produces an important stream of timely financial intelligence for FinCEN analysts and external stakeholders.

FinCEN analysts work, 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 FinCEN advisories, geographic targeting orders, and other regulatory actions; locate potential data quality issues; and flag matters that potentially exhibit behavior patterns indicative of significant money laundering activity.

For the analysis and dissemination stages of FinCEN's financial intelligence cycle, we have 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. FinCEN combines BSA data with additional information, commercial data sources, and other open source material to develop proactive targets and strategic assessments of money laundering trends and vulnerabilities for dissemination to our partners, both domestic and international.

Lastly, the financial intelligence cycle helps inform future planning and direction. Once threats and vulnerabilities have been identified, FinCEN can adjust the regulatory framework protecting the U.S. financial system. FinCEN uses its regulatory rulemaking authority to, among other things, define the reporting that financial institutions and others must provide. FinCEN also develops 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. These 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 financial intelligence activities.

Information Sharing

Financial intelligence is most effective when information flows in both directions between the public and private sectors. FinCEN serves as a communication point between financial institutions and law enforcement, regulatory, and international colleagues. Providing information to the financial industry, based on our analysis of their own reporting, is a force-multiplier.

One of the tools FinCEN uses to report suspicious behaviors possibly related to money laundering and terrorist financing threats to industry – and thus generate additional reporting that may address these suspicions – is our Financial Institution Advisory Program. FinCEN can issue public and non-public advisories to alert financial institutions of specific illicit finance risks. Advisories often contain illicit activity typologies, red flags to facilitate monitoring, and guidance on complying with FinCEN regulations to address threats and vulnerabilities. Financial institutions may use this information to enhance their AML monitoring systems for more valuable suspicious activity reporting.

The threat posed by al-Qaida, the Islamic State of Iraq and Syria (ISIS), their respective branches and affiliates, and associated foreign terrorist fighters is a key focus for FinCEN and TFI as a whole. The reporting by financial institutions is an essential component in identifying foreign terrorist fighters, financial and logistical facilitators, and their methods of moving funds. In May 2015, FinCEN issued a non-public advisory related to ISIS financing. Following the publication of the advisory, financial institutions used FinCEN's 24/7 reporting hotline to notify FinCEN of possible terrorist financing activity. This included amendments to previously reported suspicious activity where the filer had not realized at the time a potential ISIS connection, 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 with which the financial industry takes its reporting obligations.

In December 2015, FinCEN issued another non-public advisory to U.S. financial institutions, providing some "red flag" indicators to help financial institutions identify and report financial transactions that may be associated with foreign terrorist fighters who support ISIS, al-Qaida, and their affiliates in Iraq and Syria. The advisory resulted in new terrorist financing-related SARs, the amending of past SARs to indicate possible terrorist financing, and more terrorist financing tips to FinCEN's 24/7 reporting hotline.

The suspicious activity that financial institutions have identified based in part on these advisories, coupled with their own analyses, generates extremely valuable financial intelligence that FinCEN shares with our law enforcement partners.

Another useful tool for sharing information is Section 314 of the USA PATRIOT Act. FinCEN has placed significant emphasis on our public-private partnerships and on information sharing under Section 314 of the USA PATRIOT Act. Section 314(a) essentially involves sharing of information between financial institutions and government, while Section 314(b) involves sharing of information among financial institutions themselves.

FinCEN has a well-established domestic and international program implementing Section 314(a), which allows FinCEN to request certain information from financial institutions related to money laundering and terrorist financing. This authority is used to canvass the financial system

to identify accounts or transactions at the request of law enforcement. The 314(a) process has proven to be an effective tool in many law enforcement investigations with 95 percent of the 314(a) requests contributing to arrests or indictments.

Section 314(b) allows financial institutions to voluntarily share information with one another under a safe harbor that offers protections from liability in order to better identify and report potential money laundering or terrorist activities. While information sharing under the 314(b) program is voluntary, it can help financial institutions enhance compliance with their AML/CFT obligations, most notably with respect to:

- Gathering additional information on customers or transactions potentially related to money laundering or terrorist financing, including previously unknown accounts, activities, and/or associated entities or individuals;

- Shedding more light upon overall financial trails, especially if they are complex and appear to be layered amongst numerous financial institutions, entities, and jurisdictions;

- Building a more comprehensive and accurate picture of a customer's activities where potential money laundering or terrorist financing is suspected, allowing for more precise decision-making in due diligence and transaction monitoring;

- Alerting other participating financial institutions to customers whose suspicious activities those institutions may not have been previously aware;

- Facilitating the filing of more comprehensive SARs than would otherwise be filed in the absence of 314(b) information sharing;

- Identifying and aiding in the detection of money laundering and terrorist financing methods and schemes; and

- Facilitating efficient SAR reporting decisions by enabling financial institutions to obtain a more complete picture of activity through the voluntary information sharing process.

One issue frequently noted by industry regarding information sharing is the scope of their safe harbor for information sharing under Section 314(b). The statute currently provides a safe

harbor from liability for disclosing information under Section 314(b) for activities that may involve terrorist actions or money laundering activities. Activities that are the predicates for money laundering, like fraud, drug trafficking, cybercrimes, and others, are not explicitly included in the safe harbor. FinCEN issued guidance on the expansive scope of permissible information sharing covered by Section 314(b) safe harbor in 2009. .

In addition to close collaboration with domestic partners, FinCEN works to establish and strengthen mechanisms for the exchange of information globally, and to engage with, encourage, and support international partners in taking necessary steps to construct regimes to combat money laundering, terrorist financing, and other financial crimes. FinCEN responds to requests from FIUs that are members of the Egmont Group and acts as a conduit for requests from domestic law enforcement to foreign FIUs. We also proactively share information with this global network of FIUs. By leveraging the network of more than 150 FIUs globally to exchange valuable financial intelligence, we are able to work together to combat terrorist financing and money laundering threats across jurisdictional boundaries.

New and Evolving Money Laundering and Terrorist Financing Challenges

To effectively counter money laundering and the financing of terrorism, we must understand the threats, risks, and vulnerabilities posed to the U.S. and global financial systems by the broad array of illicit financial activity. We must keep a constant watch for new and emerging challenges and threats and be more creative in using our existing authorities and exploring new tools that will aid in the fight against money laundering and terrorist financing. I would like to highlight three focus areas: real estate, virtual currency, and cybersecurity.

Real Estate

FinCEN is working actively to address money laundering and terrorist financing risks in the real estate sector. FinCEN has had longstanding concerns that "all-cash" real estate transactions, i.e., those without bank financing, which are largely outside the scope of most existing AML requirements, may present money laundering vulnerabilities, particularly where a purchaser uses a shell company to conceal the true buyer. FinCEN issued Geographic Targeting Orders in January 2016 covering the Borough of Manhattan in New York, and Miami, Florida, to further

evaluate the extent of this potential money laundering vulnerability. These GTOs required certain U.S. title insurance companies to record and report the beneficial ownership information of legal entities making "all-cash" purchases of high-value residential real estate in these two geographic areas. In July 2016, FinCEN renewed the GTOs and extended coverage to additional areas in New York City, South Florida, California, and Texas. The GTOs, including the extended coverage, were renewed in February 2017.

At the time of the most recent renewal, approximately 30 percent of the real estate transactions reported under the GTOs involved a beneficial owner or purchaser representative that also had previously been the subject of a SAR. In other words, the beneficial owners or purchaser representatives in a significant portion of transactions reported under the GTO had been previously connected to suspicious activity. As a result of the attention generated by the GTOs, we have seen additional SAR filings related to potential money laundering involving real estate. In total, these SARs, along with the information generated by the GTOs, are advancing law enforcement's ability to identify potentially illicit activity and are helping inform FinCEN's broader AML approach towards the real estate sector.

While the GTO authority is a useful tool to obtain additional targeted information to inform regulatory and law enforcement efforts, there are significant limitations on the types of information that can be collected using a GTO. Under the authorizing statute, such orders may only be used to collect information on transactions involving currency or similar monetary instruments. Transactions that do not involve such instruments, such as wire transfers, may not be covered. When FinCEN works to gather information on transactions that are conducted through means other than currency or monetary instruments, as is the case with real estate transactions where the use of wires is common in many locations, the data we can gather is more limited.

Virtual Currency

The global financial industry is experiencing a period of technological innovation and growth that also creates new vulnerabilities that FinCEN and our partners must understand to prevent gaps in regulation and information collection on terrorist financing and other illicit activity.

For instance, in the virtual currency space, FinCEN has been at the forefront of engagement that balances these interests. In 2013, FinCEN released interpretive guidance on virtual currencies to provide regulatory consistency to a nascent area of the financial industry that implicated significant AML/CFT equities.

Any financial institution, payment system, or medium of exchange has the potential to be exploited for money laundering or terrorist financing. Virtual currency is not different in this regard. As with all parts of the financial system, FinCEN seeks to understand the specific attributes that make virtual currency vulnerable to illicit use, and then employ a smart regulatory approach and encourage industry to develop mitigating features in its products. Financial institutions that deal in virtual currency must put effective AML/CFT controls in place to protect themselves from illicit actors that attempt to exploit identified vulnerabilities. To that end, in May 2015, in coordination with federal law enforcement partners, FinCEN assessed the first civil monetary penalty against a virtual currency exchanger, Ripple Labs Inc., for failure to register with FinCEN as a money services business and implement and maintain an adequate AML program designed to protect its production from use by money launderers or terrorist financiers.

Cybersecurity

The size, reach, speed, and accessibility of the U.S. financial system make financial institutions attractive targets to traditional criminals, cybercriminals, terrorists, and state actors. These actors target financial institutions' websites, systems, and employees to steal customer and commercial credentials and proprietary information; defraud financial institutions and their customers; or disrupt business functions. Financial institutions play an important role in safeguarding customers and the financial system from these threats through timely and thorough reporting of cyber-events and cyber-related information in SARs. In 2016, FinCEN received more than 60,000 cyber-related SARs describing a range of cyber-enabled financial crimes.

Improved financial transparency and increased information sharing can help address the challenges posed in the cybersecurity domain. FinCEN issued an advisory in October 2016 to raise awareness among financial institutions about the intersection between cyber and AML/CFT issues. The advisory clarifies how financial institutions should approach cyber issues as they relate to SAR obligations. It also encourages coordination between AML and cybersecurity staff

to mitigate risks. In addition to the advisory, FinCEN published answers to Frequently Asked Questions concerning the filing of related SARs. We are also actively sharing indicators of suspicious cyber activity with industry, publishing more than 18,000 indicators since the launch of the program in late 2016.

In September 2016, FinCEN issued an advisory on e-mail compromise fraud schemes. It describes a variety of e-mail fraud schemes and details red flags – developed in consultation with law enforcement, including the Federal Bureau of Investigation and the U.S. Secret Service – that financial institutions may use to identify and help prevent such frauds. The schemes focus on using compromised e-mail accounts to mislead financial institutions and their customers into conducting unauthorized wire transfers. In addition to alerting industry to the types of schemes to look out for, the advisory encourages rapid communication to law enforcement when a fraudulent transaction occurs. Where U.S. businesses or financial institutions quickly alert law enforcement, FinCEN often has been able to work with its foreign counterparts to assist in the return of funds sent overseas by business email compromise schemes. Over the past two years, with respect to the illicit overseas transfer of roughly $491 million brought to our attention, we have been able to help in the return of over $275 million.

FinCEN and law enforcement agencies regularly use BSA data reported by financial institutions to initiate investigations, identify and track criminals, and disrupt and dismantle criminal networks. FinCEN strives to share actionable information with industry to help financial institutions identify and report on cyber-related suspicious activity. FinCEN will continue to share information about such threats regularly with our partners in both government and industry.

Conclusion

The current AML/CFT landscape is complex, dynamic, and requires ongoing adaptation by FinCEN and our many partners. As we continue to adjust to ever-evolving threats, we will continue to use the tools at our disposal to collect financial intelligence information, analyze it, and deploy it in support of FinCEN's mission to safeguard the financial system from illicit use, combat money laundering and terrorist financing, and promote national security.

Chairman Pearce, Vice Chairman Pittenger, Ranking Member Perlmutter, and members of the Subcommittee, thank you again for the opportunity to testify today and for your continued support of FinCEN's important mission. I look forward to your questions.