FinCEN ADVISORY

FIN-2019-A005 July 16, 2019

Updated Advisory on Email Compromise Fraud Schemes Targeting Vulnerable Business Processes

Criminals continue to exploit vulnerable business processes with business email compromise schemes – over $9 billion in possible losses affecting U.S. financial institutions and their customers since 2016.

This Advisory should be shared with:

- *Chief Executive Officers*
- *Chief Operations Officers*
- *Chief Risk Officers*
- *Chief Compliance/BSA Officers*
- *BSA/AML Analysts/Investigators*
- *Information Technology staff*
- *Cybersecurity Units*
- *Fraud Prevention Units*
- *Legal Departments*

The Financial Crimes Enforcement Network (FinCEN) is issuing this update to the "Advisory to Financial Institutions on E-mail Compromise Fraud Schemes" issued by FinCEN on September 6, 2016[1] ("2016 BEC Advisory") to alert financial institutions to predominant trends in reported business email compromise (BEC) fraud, including key sectors, entities, and vulnerable business processes targeted in many BEC schemes. This advisory (1) offers updated operational definitions for email compromise fraud; (2) provides information on the targeting of non-business entities and data by BEC schemes; (3) highlights general trends in BEC schemes targeting sectors and jurisdictions; and (4) alerts financial institutions to risks associated with the targeting of vulnerable business processes by BEC criminals. The information in this advisory, which complements the typologies and red flags identified in the 2016 BEC Advisory, may assist financial institutions in detecting, preventing, and reporting BEC fraud and associated money laundering activity. The red flags from the 2016 BEC Advisory remain relevant and can be useful to financial institutions in better identifying and reporting instances of BEC fraud.[2]

Based on FinCEN analysis of Bank Secrecy Act (BSA) data, discussions with law enforcement and other data, this advisory will assist financial institutions in recognizing and guarding against increasing email compromise fraud schemes and in considering their own or their customers'

1. *See* FinCEN Advisory FIN-2016-A003, "Advisory to Financial Institutions on E-mail Compromise Fraud Schemes," September 6, 2016.
2. For additional information regarding typologies and red flags of email compromise schemes in Suspicious Activity Reports (SARs), *see* FinCEN Advisory FIN-2016-A003, "Advisory to Financial Institutions on Email Compromise Fraud Schemes," September 6, 2016.

potential vulnerability to compromise of payment authorization and communications from email compromise fraud.[3] This advisory also highlights the potential for financial institutions to share information about subjects and accounts affiliated with email compromise schemes in the interest of identifying risks of fraudulent transactions, money laundering, and related crimes.

While the U.S. government and industry are heavily engaged in efforts to prevent email compromise fraud, reported incidents and aggregate attempted fraudulent wire amounts continue to rise. For example, the Federal Bureau of Investigation (FBI) reported over $12 billion in potential losses domestically and internationally from October 2013 to May 2018 from email compromise fraud.[4] Since the 2016 BEC Advisory was issued, FinCEN has received over 32,000 reports involving almost $9 billion in attempted theft from BEC fraud schemes affecting U.S. financial institutions and their customers. This represents a significant economic impact on the businesses, individuals, and even governments that are targeted by these schemes.

Financial institutions have provided valuable reporting to FinCEN regarding the nature and victims of email compromise schemes, some of which this advisory will highlight. Financial institutions can continue to play an important role in identifying, preventing, and reporting fraud schemes. FinCEN notes the importance of communication and collaboration among internal anti-money laundering and countering financing of terrorism (AML/CFT), compliance, business, fraud prevention, legal, and cybersecurity departments within financial institutions as well as with other financial institutions across the sector.[5] FinCEN continues to encourage this collaboration where resources and authorities permit and whenever feasible.

Updated Operational Definitions for Email Compromise Fraud

FinCEN analysis of emerging email compromise fraud typologies indicated a need to update the original definitions of email compromise fraud, BEC, and email account compromise (EAC) provided in the 2016 BEC Advisory. FinCEN broadens its definitions of email compromise fraud activities below to clarify that such fraud targets a variety of types of entities and may be used to misdirect any kind of payment or transmittal of other things of value. For example, while many email compromise fraud scheme payments are carried out via wire transfers (as originally stated in the 2016 BEC Advisory definition), FinCEN has observed BEC schemes fraudulently inducing funds or value transfers through other methods of payment, to include convertible virtual currency payments, automated clearing house transfers, and purchases of gift cards. The updated and expanded definitions below may be useful for financial institutions to consider as they refine their AML/CFT frameworks to better identify and report suspected illicit finance activity, including instances of email compromise fraud affecting transactions.

3. Aside from the updated operational definitions of email compromise fraud and business email compromise, the information in this advisory is complementary to the 2016 BEC Advisory. Financial institutions should refer to the 2016 BEC Advisory for additional information on general email account compromise (EAC) and BEC typologies and red flags.

4. *See* FBI Alert I-071218-PSA, "Business E-mail Compromise the 12 Billion Dollar Scam," July 12, 2018.

5. *See* FinCEN Advisory FIN-2016-A005, "Advisory to Financial Institutions on Cyber-Events and Cyber-Enabled Crime," October 25, 2016.

Email Compromise Fraud: Schemes in which 1) criminals compromise[6] the email accounts of victims to send fraudulent payment instructions to financial institutions or other business associates in order to misappropriate funds or value; or in which 2) criminals compromise the email accounts of victims to effect fraudulent transmission of data that can be used to conduct financial fraud. The main types of email compromise, the definitions of which have been modified to reflect the expansion of victims being targeted, include:

> ***Business Email Compromise (BEC):*** Targets accounts of financial institutions or customers of financial institutions that are operational entities, including commercial, non-profit, non-governmental, or government entities.
>
> ***Email Account Compromise (EAC):*** Targets *personal* email accounts belonging to an individual.[7]

Other Victims of BEC

FinCEN analysis has indicated criminal groups use a variety of techniques to conduct BEC fraud against individuals, particularly and increasingly those with high net worth, and entities that routinely use email to make or arrange payments between partners, customers, or suppliers. We have recently observed that targets of these schemes fall outside of the definition of traditional business customers, such as government entities and non-profit organizations or even the financial institutions themselves.

BEC Fraud against Governments

Dozens of government organizations, ranging from foreign national governments to municipal government offices, have been targets of BEC fraud. Such thefts have targeted accounts used for pension funds, payroll accounts, and contracted services, losses of which can impact government operations as well as government employees, citizens, and vendors.

Schemes against government victims are consistent with other common typologies in BEC fraud. For example, criminals hack accounts and spoof domains to send familiar-looking messages seemingly from a trusted party in the government—often someone in a leadership role in an agency or in an office that manages finances and contracts—requesting that a counterparty in the agency with the appropriate authority initiate or process a transaction. BEC schemes targeting government entities also often include vendor impersonation.

6. Criminals engaged in email compromise fraud may directly compromise email accounts through unauthorized electronic intrusions in order to leverage the compromised account for sending messages, or they may instead impersonate an email account through spoofing the email address or using an email account closely resembling a known counterparty or customer's email address (*i.e.*, that is slightly altered by adding, changing, or deleting one or more characters).
7. The definitions of email compromise fraud, BEC, and EAC supersede the definitions in the 2016 BEC Advisory.

BEC Fraud against Educational Institutions

Schools and universities, many of which are non-profit institutions, are also targets of BEC fraud. In 2016, financial institutions reported to FinCEN over 160 incidents of BEC targeting educational institutions where criminals attempted to steal over $50 million. The education sector has the largest concentration of high-value BEC attempts in financial sector reporting, even though only approximately 2% of BEC incidents affected educational institutions in 2017. Academic institutions regularly conduct or receive high dollar transactions in the form of tuition payments, endowments, grants, and renovation and construction costs, among others. This concentration of high value transactions establish both academic institutions and attending scholars as appealing targets for BEC criminals.

Schemes against educational institutions frequently involve vendor impersonation. Specifically, attackers will use compromised or spoofed email accounts to exploit existing business relationships between academic institutions and contracted service providers, such as facilities maintenance providers. Attackers use authentic-looking payment requests to direct funds to domestic bank accounts they control. Large-scale construction and renovation projects have repeatedly been targets of high-dollar thefts.

BEC Fraud against Financial Institutions

In some cases, BEC actors directly target the financial institutions themselves. This scheme typically involves spoofing bank domains and sending what appear to be credible messages to imitate official communications between bank employees, such as sending emails that appear to be from a financial institution's Society for Worldwide Interbank Financial Telecommunication (SWIFT) department with payment instructions and SWIFT reference numbers in the email text to enhance its apparent legitimacy to the victim.

Operation WireWire—Joint U.S.-International Law Enforcement Effort to Dismantle BEC Networks: In June 2018, federal authorities announced a major coordinated law enforcement effort by the U.S. Department of Justice, the U.S. Department of Homeland Security, the U.S. Department of the Treasury, the U.S. Postal Inspection Service, and international law enforcement authorities[8] to disrupt international BEC schemes and money laundering networks. The operation, called "Operation WireWire," resulted in 74 arrests across the United States and overseas, specifically, 42 arrests in the United States, 29 arrests in Nigeria, and one each in Canada, Mauritius, and Poland. Authorities seized nearly $2.4 million, and disrupted and recovered approximately $14 million in fraudulent wire transfers. U.S. law enforcement also charged 15 alleged money mules, which play a significant role in the laundering of proceeds fraudulently derived from BEC schemes, for their roles in defrauding victims in schemes targeted under Operation WireWire.[9]

8. Operation WireWire involved international cooperation between U.S. law enforcement and authorities in Canada, Indonesia, Malaysia, Mauritius, Nigeria, and Poland. *See*, FBI News, "International Business E-Mail Compromise Takedown: Multiple Countries Involved in Coordinate Law Enforcement Effort," June 11, 2018.

9. *Id*.

General Trends in BEC Schemes and Financial Flows

Financial institution reporting of suspicious activity involving BEC schemes continues to grow since the issuance of the 2016 BEC Advisory. Instances of BEC reported to FinCEN have climbed from averaging just under 500 reports per month (averaging $110 million monthly in total attempted BEC thefts) in 2016 to over 1,100 monthly reports (averaging over $300 million monthly in total attempted BEC thefts) in 2018. FinCEN analysis of sensitive financial data revealed several prominent trends in BEC schemes affecting U.S. financial institutions and their customers, including a concentration of targeting of particular sectors as well as a prevalence of BEC schemes and movement of their proceeds through several key jurisdictions.

Top Sectors Targeted in BEC

FinCEN analysis reveals that the top three sectors commonly targeted in BEC schemes are (1) manufacturing and construction (25% of reported BEC cases); (2) commercial services (18%); and (3) real estate (16%). BEC criminals are likely tailoring their methods to targeted industries in order to increase their likelihood of success. For example, BEC scams, especially those targeting financial firms,[10] continue to leverage common typologies of impersonating organization executives (otherwise known as "Chief Executive Officer [CEO] Fraud")[11] to discourage employees receiving the fraudulent payment instructions from challenging or confirming the order.

Perpetrators of BEC fraud are using fraudulent vendor invoices when targeting certain industries (such as the education sector, as described above). Fraudulent vendor and client invoices are generally affiliated with larger BEC transaction amounts than even the CEO fraud scheme, likely due to higher expected and previously recurrent transaction amounts to pay for goods and services. Additionally, vendor impersonation scams often involve foreign intermediary beneficiaries receiving the initial flow of illicit funds. BEC criminals are likely exploiting the common use of foreign vendors and attempting to reduce the likelihood of (or at least cause a delay in) financial institutions and customers recognizing the suspicious nature of the transaction.

U.S. Accounts as the Top Destinations for BEC Proceeds

The majority of BEC incidents affecting U.S. financial institutions and their customers are increasingly involving initial domestic funds transfers, rather than international, likely taking advantage of money mule networks across the United States to move stolen funds.[12] For BEC-

10. FinCEN analysis revealed that approximately half of all BEC fraud targeting financial institutions was facilitated via emails impersonating the CEO or president.

11. For specific information on this scenario in BEC fraud, refer to Scenario 2 – "Criminal Impersonates an Executive," from the FinCEN 2016 BEC Advisory.

12. In the context of this advisory, money mules refer to persons and their accounts that are used to receive and transfer illegally acquired funds, generally on behalf of or at the direction of another and can be witting or unwitting. The FBI has highlighted the role that money mules play in moving stolen funds internationally to avert the scrutiny of financial institutions and mask the identity of individuals in criminal activity, including Internet-enabled crimes. For more information, *see* FBI News, "Don't Be a Mule: FBI Joins International Campaign to Stop Money Mules," December 17, 2018.

related transactions that either initially or subsequently transfer fraudulently derived funds outside of the United States, the FBI has reported China, Hong Kong, the United Kingdom, Mexico, and Turkey as prominent destinations of BEC-derived funds.[13]

Vulnerable Business Processes Compromised[14]

BEC perpetrators continue to refine their methodologies to ensure the greatest likelihood of success, taking into consideration industry, company size, existing relationships, and potential financial counterparties in planning their schemes. BEC perpetrators identify processes vulnerable to compromise, whether through openly available information about their targets or through cyber-enabled reconnaissance efforts (enabled through methods such as spear phishing or malware), and then insert themselves into communications by impersonating a critical player in a business relationship or transaction.[15] A scheme's probability of success and the potential payout from fraudulent payment instructions often depends on the criminal's knowledge of their victim's normal business processes, as well as weaknesses in the victim's authorization and authentication protocols.

Industries with public-facing information about their business transactions and processes can present attractive targets for BEC schemes. Such schemes have targeted the education, real estate, and agriculture sectors by leveraging publicly available information about the victim organization's vendors, contracts, and business processes.

Business Process Compromise Example—BEC Targeting Real Estate Transactions: Real estate transactions have been a particularly lucrative target for BEC schemes. The large dollar volumes involved in such transactions, whether for down payments on a property or the final transfer of proceeds upon closing, are an attractive target of opportunity for criminals engaged in BEC activity. FinCEN analysis reveals that BEC criminals often targeted several potential vulnerabilities of common real estate-related business processes:

a) Readily availability detailed public information regarding potential real estate transactions and counterparties (*e.g.*, real estate agents and homeowners);

b) General communication of transactions between real estate counterparties conducted via email; and

c) A common lack of strong authentication processes for verifying identity and validity of instructions in associated communications.

13. *See* FBI Alert I-071218-PSA, "Business E-mail Compromise the 12 Billion Dollar Scam," July 12, 2018.

14. The term "business processes" here refers to activities, protocols, and systems that support an organization's line of business and could be used in the conduct, facilitation, or affecting of transactions. This can include an organization's communications methods and schedules of transmitting payment information and the organization's payment authorization and authentication processes.

15. BEC perpetrators may leverage cyber-enabled reconnaissance efforts such as skillful social engineering or computer intrusions to gain sufficient knowledge of the organizations' business processes.

Communications that integrate publicly available information with private information obtained via email compromise can be extremely effective in fraudulently inducing an individual to send wires to accounts controlled by a BEC criminal. By understanding the nature of these social engineering schemes and assessing and mitigating their business process vulnerabilities to compromise, financial institutions and their customers can reduce their susceptibility to BEC fraud.

BEC Data Theft

As financial institutions consider their risk from BEC fraud, they should also consider their authentication and authorization processes for receiving sensitive data about the organization or their customers. The FBI and FinCEN have noted that email compromise scams have been used to deceive victims into providing criminals with protected information, such as Personally Identifiable Information (PII) or Wage and Tax Statement (W-2) forms for a business's employees.[16] Criminals often use stolen information in future fraudulent transactions, account takeovers, or other crimes.

Opportunities for Information Sharing Related to BEC Fraud

Many beneficiaries of BEC schemes play roles in larger networks of criminal activity and laundering of funds from illicit activity. Under the USA PATRIOT Act 314(b) safe harbor protections,[17] financial institutions may share information surrounding BEC fraud for purposes of identifying and, where appropriate, reporting activities that they suspect may involve possible terrorist activity or money laundering.[18] Such information sharing may assist fellow institutions in identifying risks to the industry amounting to billions of dollars.

Since November 2016, financial institutions reported over 6,000 instances and over $2.6 billion in attempted and successful transactions affiliated with suspected money laundering activity through BEC schemes. FinCEN encourages financial institutions to share valuable information about BEC beneficiaries and perpetrators, for purposes of identifying and, where appropriate, reporting activities that they suspect may involve possible terrorist activity or money laundering. Doing so may also help protect those institutions and their customers from facing the devastating losses often caused by these schemes and help identify and prevent financial crime and movement of funds through broader criminal money laundering networks.

16. For the FBI's latest Public Service Announcement on email compromise fraud, *see* FBI Alert I-071218-PSA "Business E-mail Compromise the 12 Billion Dollar Scam," July 12, 2018.

17. *See* Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 ("USA PATRIOT Act") Pub. L. No. 107-56, § 314(b); and 31 CFR § 103.110(b)(5).

18. For FinCEN's guidance clarifying that 314(b) participants may share information related to transactions, as well as the underlying specified unlawful activities, under the protection of the 314(b) safe harbor if the participant suspects that transactions may involve the proceeds of specified unlawful activities under money laundering statutes, *see* FinCEN Guidance FIN-2009-G002 "Guidance on the Scope of Permissible Information Sharing Covered by Section 314(b) Safe Harbor of the USA PATRIOT Act," June 16, 2009.

Information for U.S. Financial Institutions[19]

Risk Management Considerations

FinCEN encourages financial institutions and their customers to assess the vulnerability of their business processes to compromise and consider if there are appropriate steps within their risk management approach to "harden" or increase the resiliency of their processes and systems against email fraud schemes. This can include considering the risk surrounding the financial institutions' or organizations' business processes and practices to 1) authenticate participants in communications, 2) authorize transactions, and 3) communicate information and changes about transactions.[20] The FBI has posted suggestions for internal protection techniques against email compromise fraud schemes that have been highly successful in recognizing and deflecting BEC/EAC attempts. Considering these steps could assist financial institutions in identifying and preventing transactions not authorized by their customers but requested fraudulently in BEC schemes that communicate directly with the financial institution.

A multi-faceted transaction verification process, as well as training and awareness-building to identify and avoid spear phishing schemes, can help financial institutions guard against BEC and EAC fraud. For instance, financial institutions may verify the authenticity of suspicious emailed transaction payment instructions by using multiple means of communication or by contacting others authorized to conduct the transactions. The success of BEC and EAC schemes depends on criminals prompting financial institutions to execute seemingly legitimate but unauthorized or fraudulently induced transactions. Such transactions are often irrevocable, which renders financial institutions and their customers unable to cancel payments or recall the funds. Identifying fraudulent transaction payment instructions before payments are issued is therefore essential to preventing and reducing unauthorized transactions.

Response and Recovery of Funds

FinCEN, in partnership with the FBI, the U.S. Secret Service (USSS), HSI, and the U.S. Postal Inspection Service, as well as counterpart Financial Intelligence Units (FIUs) abroad, can help financial institutions recover funds stolen as the result of BEC schemes through its Rapid Response Program (RRP). Through these partnerships, FinCEN has successfully assisted in the recovery of over $515 million with the assistance of 64 countries. While the recovery of BEC stolen funds is not assured, **FinCEN has had greater success in recovering funds when victims or financial institutions report BEC-unauthorized and fraudulently induced wire transfers to law enforcement within 24 hours**.

19. This section supersedes the information for financial institutions in the 2016 BEC Advisory. The information in this section is consistent with that in the previous advisory but includes updated elements to account for trends FinCEN identified in the email compromise fraud reporting.

20. In considering the risk of their institution or organization's business processes to compromise by BEC, entities should consider the level of information available publicly about key financial counterparties and processes, including information on public websites or on the darknet (*e.g.*, email account login credentials that have been compromised and posted for sale).

To request immediate assistance in recovering BEC-stolen funds, financial institutions should file a complaint with the FBI's Internet Crime Complaint Center (IC3), contact their local FBI field office, or contact the nearest USSS field office. Contacting law enforcement for fund recovery assistance does not relieve a financial institution from its Suspicious Activity Report (SAR) filing obligations.

Information Sharing

Due to the nature of BEC and EAC schemes, FinCEN encourages communication among financial institutions under the auspices of Section 314(b) of the USA PATRIOT Act for purposes of identifying and, where appropriate, reporting activities that they suspect may involve possible terrorist activity or money laundering. Sharing of this information could also help prevent billions of dollars in potential losses to financial institutions and their customers. Financial institutions should be prepared to provide transactional details and cyber-related information surrounding the BEC scheme when requesting assistance in recovering funds.

Suspicious Activity Reporting

A financial institution is required to file a SAR if it knows, suspects, or has reason to suspect a transaction conducted or attempted by, at, or through the financial institution involves or aggregates to $5,000 or more in funds or other assets and involves funds derived from illegal activity, or attempts to disguise funds derived from illegal activity; is designed to evade regulations promulgated under the BSA; lacks a business or apparent lawful purpose; or involves the use of the financial institution to facilitate criminal activity.[21] With respect to email compromise fraud involving fraudulent payment instructions, a financial institution has a SAR filing obligation regardless of whether the scheme or involved transactions were successful, and regardless of whether the financial institution or its customers incurred an actual loss.[22]

Financial institutions are required to file complete and accurate reports that incorporate **all relevant information** available, including **cyber-related information**. When filing a SAR regarding suspicious transactions that involve cyber-events (such as BEC fraud), financial institutions should provide all pertinent available information on the event and associated suspicious activity, including cyber-related information, in the SAR form and narrative.[23] Specifically, the following information is highly valuable to law enforcement and FinCEN in investigating BEC/EAC fraud:

21. *See*, 31 CFR. §§ 1020.320, 1021.320, 1022.320, 1023.320, 1024.320, 1025.320, 1026.320, 1029.320, and 1030.320. The monetary threshold for filing money services businesses SARs is, with one exception, set at or above $2,000 (*see* 31 CFR. § 1022.320(a)(2)).
22. *Id*.
23. *See* FinCEN Frequently Asked Questions, "Frequently Asked Questions (FAQs) regarding the Reporting of Cyber-Events, Cyber-Enabled Crime, and Cyber-Related Information through Suspicious Activity Reports (SARs)," October 25, 2016.

Transaction details:

1) Dates and amounts of suspicious transactions;
2) Sender's identifying information, account number, and financial institution;
3) Beneficiary's identifying information, account number, and financial institution; and
4) Correspondent and intermediary financial institutions' information, if applicable.

Scheme details:

1) Relevant email addresses and associated Internet Protocol (IP) addresses with their respective timestamps;
2) Description and timing of suspicious email communications and any involved compromised or impersonated parties; and
3) Description of related cyber-events and use (or compromise) of particular technology in the conduct of the fraud. For example, financial institutions should consider including any of the following information or evidence related to the email compromise fraud:
   a) Email auto-forwarding
   b) Inbox sweep rules or sorting rules set up in victim email accounts
   c) A malware attack
   d) The authentication protocol that was compromised (*i.e.*, single-factor or multi-factor, one-step or multi-step, etc.)

FinCEN continues to encourage financial institution collaboration among BSA/AML, cybersecurity, legal departments, fraud prevention, and other relevant units that can assist financial institutions to identify and report relevant technical indicators and other information related to cyber-events and cyber-enabled crime, including email compromise fraud schemes.[24]

The trends and typologies reported in this advisory, in conjunction with the red flags and other information in the 2016 BEC Advisory, should assist financial institutions in better identifying BEC-related activity and risk. As with red flags, financial activity involving the highlighted sectors and jurisdictions in this advisory associated with higher levels of BEC and EAC fraud

24. *See* FinCEN Advisory FIN-2016-A005, "Advisory to Financial Institutions on Cyber-Events and Cyber-Enabled Crime," October 25, 2016.

may actually reflect legitimate financial activities, therefore financial institutions should evaluate indicators of potential BEC or EAC activity in combination with other red flags and the expected transaction activity before making determinations of suspiciousness.[25]

FinCEN requests that financial institutions **reference this advisory and include the following key terms in the SAR narrative**:

"BEC FRAUD" when **businesses or organizations** are the scheme victims

"EAC FRAUD" when **individuals** are the scheme victims

Financial institutions should also select SAR field 42 (Cyber event) as the associated suspicious activity type to indicate a connection between the suspicious activity being reported and possible BEC or EAC fraud. Financial institutions should include one or both key terms to the extent they are able to distinguish between BEC and EAC fraud. Additionally, financial institutions **should include any relevant technical cyber indicators** related to the email compromise fraud and associated transactions **within the available structured cyber event indicator SAR fields 44(a)-(j), (z)**.

In instances of **reporting of BEC** schemes that **result in the communication of *information*** that could be used to facilitate future fraudulent transactions, which may be voluntary, FinCEN requests that financial institutions include the following key term in the SAR narrative:

"BEC DATA THEFT"

This advisory does not establish new regulatory interpretations, expectations, or requirements. The obligations of regulated persons and financial institutions under the Bank Secrecy Act are subject to the applicable sections of the Code of Federal Regulations, and to subsequent administrative rulings that clarify the application of the rules within the context of specific sets of facts and circumstances. All definitions proposed in this advisory are for ease of reference only, and apply only within the scope of the advisory itself.

25. For additional information regarding typologies and red flags of email compromise schemes in Suspicious Activity Reports (SARs), *see* FinCEN Advisory FIN-2016-A003, "Advisory to Financial Institutions on Email Compromise Fraud Schemes," September 6, 2016.

For Further Information

Additional questions or comments regarding the contents of this advisory should be addressed to the FinCEN Resource Center at frc@fincen.gov.

Financial institutions wanting to report suspicious transactions that may potentially relate to terrorist activity should call the Financial Institutions Toll-Free Hotline at (866) 556-3974 (7 days a week, 24 hours a day). The purpose of the hotline is to expedite the delivery of this information to law enforcement. Financial institutions should immediately report any imminent threat to local-area law enforcement officials.

The mission of the Financial Crimes Enforcement Network is to safeguard the financial system from illicit use, combat money laundering, and promote national security through the strategic use of financial authorities and the collection, analysis, and dissemination of financial intelligence.