EGMONT GROUP BULLETIN

Business Email Compromise Fraud

Information Exchange Working Group

IEWG

July 2019
- Public version-

THE EGMONT GROUP OF FINANCIAL INTELLIGENCE UNITS

PUBLIC BULLETIN: BUSINESS E-MAIL COMPROMISE FRAUD

The purpose of this bulletin is to alert competent authorities and reporting entities of key typologies and money laundering risks associated with business e-mail compromise (BEC) fraud schemes. The information in this bulletin should assist authorities and reporting institutions to better detect, identify, report, and investigate BEC fraud schemes and disrupt these illicit finance networks.

BULLETIN ON BUSINESS E-MAIL COMPROMISE FRAUD

Identification number: EG-Bulletin-01/2019
Date: July 30, 2019
Intended Recipients: Competent Authorities (Regulatory, Supervisory, and Law Enforcement), and Reporting Entities

Introduction

Preventing cyber criminals from exploiting the global financial system is a key priority for the Egmont Group of Financial Intelligence Units (FIUs) and its members. The Egmont Group is issuing this bulletin to alert member FIUs and their jurisdictions of the increasing threat posed by BEC fraud schemes. BEC fraud schemes are among the fastest-growing cyber-enabled crime threats adversely affecting financial institutions, exposing the financial sector to billions of dollars in losses worldwide. For example, one jurisdiction identified over $12 billion in potential losses from over 78,000 reported incidents of BEC fraud, during a recent five-year period, involving victims domestically and internationally.[1] These schemes target business organizations, professionals, and individuals by compromising either business or personal email accounts to send (or cause to be sent) false payment instructions and other information used to conduct financial fraud.

Business E-mail Compromise Fraud

BEC fraud involves schemes in which criminals compromise the e-mail accounts of victims either to (1) send fraudulent payment instructions to financial institutions or other business associates in order to misappropriate funds; or (2) cause data to be transmitted fraudulently to conduct financial fraud.

Financial institutions can play an important role in identifying, preventing, and reporting BEC fraud schemes by promoting greater communication and collaboration among their internal anti-money laundering (AML), business, fraud prevention, and cybersecurity units.

To address the increasing and serious threat posed by BEC to financial institutions and their customers, 11 FIUs launched the Egmont BEC Project Team, which is focused on analyzing BEC trends and methodologies. The Egmont Group's objective is to share key findings of this analysis with FIUs, in the hope that the FIUs will share, as appropriate, the information with

[1] *See* Federal Bureau of Investigation (FBI) Public Service Announcement, *Business Email Compromise: The 12 Billion Dollar Scam*, July 12, 2018, available at https://www.ic3.gov/media/2018/180712.aspx.

competent authorities and reporting institutions. Based on these key findings, this Bulletin contains indicators of BEC schemes and associated fraudulently-induced transactions. Reporting institutions receiving this Bulletin may use it to identify and report possible BEC-related transactions to competent regulatory, supervisory, and law enforcement authorities.

How BEC Schemes Work

BEC schemes generally involve impersonating victims to submit seemingly legitimate transaction instructions for a financial institution to execute. While BEC schemes differ in certain aspects, they all focus on using compromised e-mail accounts to cause financial institutions and/or their customers to make unauthorized or fraudulently-induced payments or to send sensitive data to an unauthorized third party, which then uses such data to conduct financial fraud. BEC schemes can be broken down into three stages:

Stage 1 – Compromising Victim Information and E-mail Accounts: Criminals first unlawfully access a victim's e-mail account, often through social engineering[2] or computer intrusion techniques. Criminals subsequently exploit the compromised e-mail account to obtain information on the victim's financial institutions, account details, contacts, and related information.

Stage 2 – Transmitting Fraudulent Transaction Instructions: Criminals then use the victim's stolen information to e-mail fraudulent payment or data transmission instructions to the financial institution, in a manner appearing to be from the victim. To this end, criminals will use either the victim's actual e-mail account they now control or create a fake e-mail account resembling the victim's e-mail. To support their instructions, the criminal may provide supporting documents, falsified for this purpose to enhance their apparent legitimacy.

Stage 3 – Executing Unauthorized Transactions: Criminals trick the victim's employee or financial institution into conducting money transfers that appear legitimate but are, in fact, unauthorized or fraudulently-induced. The fraudulent transaction instructions direct the payments to the criminals' accounts at domestic or foreign financial institutions. Financial institutions in East and Southeast Asia as well as Western and Eastern European countries are common destinations for these fraudulent transactions. However, it should be noted that criminals often adapt their strategies and that destination countries can change quickly.

BEC Scenarios

BEC schemes often target financial institutions or their customers, including businesses and individuals, who conduct large transactions through financial institutions, lending entities, real estate companies, and law firms. To illustrate, BEC schemes often take the following forms:

Scenario 1 – Criminal Impersonates a Financial Institution's Commercial Customer: A criminal hacks into and uses the e-mail account of a Company A employee to send fraudulent wire transfer instructions to Company A's financial institution.[3] Based on this request,

[2] Social engineering refers to human interaction tactics used to deceive an individual into revealing information. Criminals primarily use social engineering to facilitate BEC fraud schemes.

[3] In all of these scenarios, rather than hacking into an account, the criminal may also simply spoof the email address or create an email account that closely resembles the legitimate email address of the requesting party.

Company A's financial institution issues a wire transfer and sends funds to an account the criminal controls.

In this scenario, the criminal, impersonating the financial institution's customer, prompts the financial institution to execute an unauthorized wire transfer.

Scenario 2 – Criminal Impersonates an Executive (a.k.a. "CEO Fraud"): A criminal hacks into and uses the e-mail account of a Company B executive to send wire transfer instructions to a Company B employee, who is responsible for processing and issuing payments. The employee, believing the executive's e-mailed instructions are legitimate, orders Company B's financial institution to execute the wire transfer.

In this scenario, the criminal impersonating a company executive misleads a company employee into unintentionally authorizing a fraudulent wire transfer to a criminal-controlled account. *Other variations of this scenario can include a criminal impersonating a company executive to mislead a company employee into sending sensitive payroll or transaction information that the criminal can use in future financial fraud.*

Scenario 3 – Criminal Impersonates a Supplier: A criminal impersonates one of Company C's suppliers or a professional services provider (such as a real estate agent, escrow company, or attorney) to e-mail and inform Company C that future invoice payments or deposits should be sent to a new account number and location. Based on this fraudulent information, Company C updates its supplier's payment information on record and submits the new wire transfer instructions to its financial institution, which then directs payments to an account controlled by the criminal.

In this scenario, the criminal, impersonating a supplier or service provider, sends fraudulent payment information to mislead a company employee into directing wire transfers to a criminal-controlled account.

Scenario 4 – Criminal Targets Real Estate Services: A criminal compromises the e-mail account of a real estate agent or of an individual purchasing or selling real estate, for the purposes of altering payment instructions and diverting funds of a real estate transaction (such as sale proceeds, loan disbursements, or fees). Alternately, a criminal hacks into and uses a real estate agent's e-mail address to contact an escrow company, instructing it to redirect commission proceeds that the real estate agent earns for the sale of the property to an account controlled by the criminal.

In this scenario, the criminal impersonates a real estate agent or another key participant in the real estate transaction to send fraudulent payment instructions that mislead a counterparty into directing down payments or other real estate transaction-related funds into a criminal-controlled account.

BEC Fraud Indicators

Success in detecting and stopping BEC schemes requires careful review and verification of customers' transaction instructions and consideration of the circumstances surrounding such instructions. Because some indicators associated with BEC fraud may actually reflect legitimate financial activities, financial institutions are advised that ***no single transactional indicator necessarily indicates suspicious activity***. Financial institutions should consider additional indicators and the surrounding facts and circumstances, such as a customer's historical financial activity and whether the customer exhibits multiple indicators, before determining that a transaction is suspicious. Financial institutions should also perform additional inquiries and investigations where appropriate.

The following indicators may indicate a BEC scheme:

Victim Account Indicators

General Suspicious Transaction Patterns

- A customer e-mails transaction instructions that direct payment to a known beneficiary; however, the beneficiary's account information is different from that previously used.
- A customer e-mails transaction instructions that direct payment to a beneficiary with which the customer has no payment history or documented business relationship, and the payment is in an amount similar to or in excess of payments previously sent from the customer to beneficiaries.
- A customer e-mails transaction requests for additional payments immediately following a successful payment to an account not previously used by the customer to pay its suppliers/vendors. Such behavior may be consistent with a criminal attempting to issue additional unauthorized payments after learning that a fraudulent payment was successful.
- A customer e-mails transaction instructions that purport to designate the transaction request as "Urgent," "Secret," or "Confidential."
- A customer e-mails transaction instructions in a manner that would give the financial institution limited time or opportunity to confirm the authenticity of the requested transaction.
- A customer e-mails transaction instructions to direct wire transfers to a foreign financial institution account that has been documented in customer complaints as a suspected destination of fraudulent transactions.
- A customer's seemingly legitimate e-mailed transaction instructions contain different language, timing, and amounts than previously verified and authentic transaction instructions.

- Transaction instructions originate from an e-mail account closely resembling a known customer's e-mail account; however, the e-mail address has been slightly altered by adding, changing, or deleting one or more characters. For example:

Legitimate e-mail address	Fraudulent e-mail addresses
john-doe@abc.com	john_doe@abc.com john-doe@bcd.com

- A financial institution receives e-mailed transaction instructions from a customer's employee, who is a newly-authorized person on the account, or is an authorized person, who has not previously sent wire transfer instructions.
- A customer's employee or representative e-mails a financial institution transaction instructions on behalf of the customer that are based exclusively on e-mail communications originating from executives, attorneys, or their designees. However, the customer's employee or representative indicates he/she has been unable to verify the transactions with such executives, attorneys, or designees.

High Risk Jurisdictions for BEC

- The beneficiary's account may belong to an offshore company or be held by a financial institution located in a high-risk jurisdiction, as determined by the financial institution and the institution's relevant jurisdictional competent authorities.

Use of Forged Documents or Invoices

- Criminals send forged documents or invoices to a victim's employee to confirm the transaction. Forged documents and invoices can be of high quality and may even include genuine documents that have been modified to divert money to a criminal's financial institution account.

Indicators Involving the Account of Suspected BEC Criminals

General Suspicious Transaction Patterns

- After an attack on an account/company, funds are immediately withdrawn from the financial institution, immediately transferred out of the financial institution, or are transferred to multiple accounts within the financial institution.
- A financial institution receives a wire transfer for credit into an account, however, the wire transfer names a beneficiary that is not the account holder of record. This may reflect instances where a victim unwittingly sends wire transfers to a new account number, provided by a criminal, impersonating a known supplier/vendor, while thinking the new account belongs to the known supplier/vendor, as described in the above BEC Scenario 3. This indicator may be seen by financial institutions receiving wire transfers sent by another financial institution as the result of BEC fraud.

Amount of Transfer

- The amount of a funds transfer received in the beneficiary's account is not in line with the customer's profile.

Use of Money Mules

- The sudden increase in large transactions and balances of an intermediary customer can indicate potential participation as a money mule in a BEC fraud scheme. Money mules[4] serve as intermediaries for criminals and criminal organizations. In some cases, victims are unaware that they are being used to fraudulently transport money to cyber criminals. Criminals commonly use money mules to carry out BEC-related fraud schemes. Money mules generally maintain low balances or have limited financial activity prior to becoming involved in the scheme.

Risk Mitigation

A multi-faceted transaction verification process can help financial institutions guard against BEC fraud. For instance, financial institutions may verify the authenticity of suspicious e-mailed transaction payment instructions by communicating with the customer through multiple means (e.g., telephone, alternative email accounts), or by contacting others in the customer's company who are authorized to conduct the transactions. The success of BEC schemes depends on criminals prompting financial institutions to execute seemingly legitimate but unauthorized transactions. Such transactions are often irrevocable, which renders financial institutions and their customers unable to cancel payment or recall the funds. Identifying fraudulent transaction payment instructions before payments are issued is therefore essential to preventing and reducing unauthorized transactions.

Responding to BEC Incidents and Recovering Funds

Some members of the Egmont Group of FIUs work collaboratively with financial institutions and law enforcement to help recover funds for victims by quickly disseminating information related to suspected financial fraud tied to BEC. Quick action on the part of victims, financial institutions, and law enforcement is critical to the successful recovery of victim funds. The recovery rate of funds lost to BEC drops significantly after the first 24 hours.

To assist in the investigation of BEC incidents and recovery of victims' funds from BEC-related fraud, financial institutions are advised to take the following steps:[5]

1) **Contact Law Enforcement and Other Competent Authorities Immediately**

   a. *Report the Crime:* It is imperative that the victim, financial institutions, law enforcement, regulatory, and the national and foreign FIUs act swiftly in their

[4] The identity of money mules is used to open financial institution accounts, obtain bank cards with a PIN, obtain personalized codes, and attain access to online payment facilities. Money mules must hand over this information or transfer their access to other members of the organized criminal group for criminal use. Money mules usually have no idea about the greater picture of the crime in which they participated and only receive a small amount for the "service" provided.

[5] The components of each step are not necessarily sequential in nature, as many of these activities can occur concurrently or in close succession. As indicated above, timeliness in response and cooperation with competent authorities, including law enforcement and FIUs, are key in supporting recovery of funds lost to BEC.

attempt to recover the wired funds. To do this, the victim or the victim's financial institution must make an immediate report of the crime and request assistance from law enforcement and the FIU.[6]

Note that it is also important for financial institutions to report not only successful transactions but also unsuccessful attempts, as information surrounding the attempted fraud can still be critical in supporting competent authorities in investigating illicit activity and criminal networks.

b. *Alert the Beneficiary Financial Institution:* the financial institution holding the victim's account should immediately contact the beneficiary financial institution to inform it about the suspicion of fraud.

c. *Flag a Suspicious Incoming Transaction:* The financial institution of the potential criminal or initial beneficiary of the fraudulently-induced funds may suspect fraud if it has doubts about the lawful origin of received funds. In this case, the financial institution should immediately contact its jurisdiction's relevant regulatory, and law enforcement authorities, and FIU to alert them of the suspicious transaction.

The reporting entity should also immediately file a Suspicious Transaction Report (STR) with the relevant FIU, as appropriate. If the transfer has been executed within the last 72 hours, the person that files the complaint should insist on the urgency of the situation.

2) Stop the Movement of Currency

a. *Do Not Carry Out Suspicious Transactions:* The beneficiary financial institution that has information (e.g., SWIFT recall message) that a fraudulent transfer was executed on the account of one of its customers should not carry out transactions that could lead to the loss of the funds. In order to assess the validity of the received transaction, the beneficiary financial institution should contact law enforcement and the FIU.

3) Seize/Recover the Assets

a. *Informing Competent Authorities of Asset Locations:* To increase the likelihood of asset recovery, financial institutions should cooperate with law enforcement and their local FIU, by providing all information requested. Financial institutions should inform the FIU and law enforcement before executing any outgoing transaction, if the funds are still in the account, as well as provide information on the next destination of the funds that have already been transferred out of the account.

b. *Freeze Orders:* Financial institutions should cooperate with the FIU and/or law enforcement in the case of freeze orders issued by competent authorities.

[6] The authority and operation of law enforcement, FIUs, and other competent authorities vary by jurisdiction. Though this section highlights the importance of taking action to inform both law enforcement and local FIUs in cases of BEC schemes, affected persons and financial institutions should take into consideration the relevant authorities within their jurisdiction to determine the appropriate entities for outreach.

Suspicious Transaction Reporting Based on this Bulletin

With respect to the procedure applicable in their jurisdiction, reporting institutions should reference this Bulletin when reporting potential BEC-related transactions based on this Bulletin's indicators to their jurisdiction's relevant competent authorities. Referencing this Bulletin in STRs will allow the relevant competent authorities to identify and take steps to assist in recovering funds and investigating BEC-related fraud. Reporting entities should consider, where possible, including the following key term in their STR reporting to indicate having referenced this Bulletin in identifying suspicious transactions that may be related to BEC schemes:

"Egmont BEC Bulletin"

Institutions reporting e-mail compromise fraud through STRs are reminded to include all relevant and detailed information as is permissible, especially the following:

Wire transfer details:

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

Scheme details:

- Cyber indicators, such as relevant e-mail addresses, email headers, and associated Internet Protocol (IP) addresses with their respective timestamps; and
- Description and timing of suspicious e-mail communications.