Tips on Safeguarding Your Bank and Customers from Business E-mail Compromise (BEC) Scams

15 October 2019

TLP GREEN

This paper is marked as traffic light protocol (TLP) "GREEN". As such, recipients may share this information with peers, trusted government and critical infrastructure partner organizations, and service providers with whom they have a contractual relationship, who have a need-to-know basis. This paper should not be shared publicly.

What is a Business Email Compromise Scam

"Business Email Compromise" (BEC) is a sophisticated scam which targets both businesses and individuals performing wire transfer payments. The scam is frequently carried out when a subject compromises legitimate business e-mail accounts through social engineering or computer intrusion techniques to conduct unauthorized transfers of funds. The scam primarily involves a request to transfer funds via wire transfers, automated clearing house transfers, gift cards, and convertible virtual currency payments. However, there are variations of the scam that involves compromising legitimate business e-mail accounts and requesting Personally Identifiable Information (PII) or Wage and Tax Statement (W-2) forms for employees. The following figure explains how fraudsters conduct BEC fraud. What makes BEC such a successful fraud scheme is that threat actors utilize intercepted information that is both privileged and contemporaneous. This information is vital and very effective to induce the victim to send the unauthorized transfer of funds.

Figure 1. Wire fraud scam workflow

BEC Scams Can Destroy Trusted Relationships

The ripple effect of a successful BEC attack goes far beyond any financial impact. Generational relationships once built upon trust and confidence can deteriorate and become adversarial in an effort to recover lost monies. Your customers are not the only ones impacted. A BEC event can also trigger a series of events including compliance, financial, legal, regulatory, and reputational complications.

Tips on Identifying Spoofed Emails

Many spoofed emails are difficult to detect. However, there are several tips for identifying spoofed emails. First, carefully look at the email to identify irregularities. While one error may not constitute a spoofed email, observing multiple errors should raise additional caution requiring further research such as. The example of a phishing email shown in *Figure 2* reveals several "red flags" which can alert the reader if they stop, think and then click.

"Red flags" include:

1) Irregular time and format uncommon for the US
2) Poor grammar and spelling
3) Sense of urgency
4) Examining the source code embedded in the email reveals the actual email address is rchue@gmail.com and no rblackmore@ninebank.com

Date: Mon, 4 Jan 2019 22:18:08 GMT
From: CEO Name <rblackmore@ninebank.com>
To: Accounting@ninebanks.com
Subject: Please get back to me on this
Do you have a moment? I am tied up in a meeting and there is something i need you to take care of.
We have a pending invoice from our Vendor. I have asked them to email me a copy of the invoice and i will appreciate it if you can handle it before the close of banking transactions for today.
I cant take calls now so an email will be fine.
R.
Sent from my iPhone

Figure 2. Example of initial spoofed email.

Follow-up emails by BEC scammers are designed to be authoritative and provide instructions for performing the wire transfer.

1) Many of the same irregularities appear on subsequent emails.
2) In this example, the wire transfer comes at timeframe inconsistent with where your offices are located or where your bank's CEO may be.
3) An attachment is also included in the email. Opening attachments on emails such as this can be a mistake as it may contain malicious code.

Date: Fri, 9 Jan 2019 23:46:22 GMT
From: Richard Blackmore [rblackmore@ninebank.com]
To: Accounting@ninebanks.com
Subject: Please get back to me on this

I'm following up on my early email. The invoice is attached i mentioned. I authorize you to wire transfer $598,000 to the vendor. Account and wire instructions are on the invoice. Confirm me when it's been sent. Thanks for doin this.
R.
Sent from my iPhone

PDF
JAC Marketing

Figure 3. Example of spoofed email requesting the wire transfer.

Risk Mitigation

The first step in mitigating the risk of fraud from a BEC scam is to understand the criminal's techniques. The second step is to deploy effective payment risk mitigation processes. There are

various methods to reduce the risk of falling victim to this scam and subsequently executing a fraudulent wire transfer. Some of these methods include:

- VERIFICATION. Verify changes in payment instructions to a vendor or supplier by calling to verbally confirm the request (the phone number should not come from the electronic communication, but should instead be taken from a known contact list for that vendor);
- CONTACT INFORMATION: Maintain a file, preferably in non-electronic form, of vendor contact information for those who are authorized to approve changes in payment instructions;
- AUTHORITY CONTROLS: Limit the number of employees within a business who have the authority to approve and/or conduct wire transfers;
- AUTHENTICATION: Use out of band authentication to verify wire transfer requests that are seemingly coming from executives. This may include calling the executive to obtain verbal verification, establishing a phone Personal Identification Number (PIN) to verify the executive's identity, or sending the executive via text message a one-time code and a phone number to call in order to confirm the wire transfer request;
- DELAY UNTIL VERIFIED: When the staff at a victim business is contacted by the bank to verify the wire transfer, the staff should delay the transaction until additional verifications can be performed; and
- DUAL APPROVAL: Require dual approval for any wire transfer request involving:
    - A dollar amount over a specific threshold; and/or
    - Trading partners who have not been previously added to a "white list" of approved trading partners to receive wire payments; and/or
    - Any new trading partners; and/or
    - New bank and/or account numbers for current trading partners; and/or
    - Wire transfers to countries outside of the normal trading patterns.

The second step in risk mitigation is to strengthen protection of information, particularly financial information. As stated earlier threat actors use intercepted privileged and contemporaneous information to induce the fraudulent transfers of funds. This information is intercepted through email systems. Specifically, threat actors will penetrate a victim's email system and install auto-forwarding and/or filter rules to monitor surreptitiously victim email accounts. Having strong protections, alerts, and monitoring of changes to email systems can help to alleviate the risk of privileged and contemporaneous information from being used to perpetuate a BEC incident.

Importance of a Robust Incident Response Plan

To protect financial institutions from threats and financial fraud, regulatory agencies require each institution to have a written incident response plan in place.[1] To create an incident response plan, consider these four elements:

1. Prepare and Plan
2. Detection and Analysis
3. Containment, Eradication, and Recovery
4. Review and Update Plan

Figure 4: Incident Response Lifecycle

Also, be sure to:

- Review and obtain executive approval
- Define roles and responsibilities who has delegated authority if key people are not available (See [2]FDIC)
- Establish an internal communication tree
- Test your incident response process (ongoing); apply lessons learned[3]

Tips on Recovering Funds

Following identification of the fraud, seek to recall the wire transfer as quickly as possible by doing the following:

1. Document actions related to the incident as they occur for evidentiary purposes then filing a report with law enforcement
2. Follow SWIFT's wire transfer recall process
3. Prepare and have the victim organizations legal documentation signed and available to be sent to the recipient wire transfer institution (e.g. Unauthorized Electronic Fund Transfer Affidavit of Fraud and Hold Harmless or Letter of Indemnity)
4. Identify fraud counterpart and notify them of the fraud[4]
5. Provide the legal document to correspondent institution

[1] FFIEC Handbook: https://ithandbook.ffiec.gov/it-booklets/information-security/iii-security-operations/iiid-incident-response.aspx
[2] https://www.fdic.gov/regulations/resources/director/technical/cyber/cyber.html
[3] The FS-ISAC hosts several exercises that banks can leverage. See fsisac.com/exercises. Additionally, the FDIC publishes cyber vignettes specifically for community institutions which can be found at the Director's Resource Center.

6. Monitor and follow-up
    - Regulatory Reporting
    - Never make any payment changes without verifying with the intended recipient; verify email addresses are accurate when checking mail on a cell phone or other mobile device.

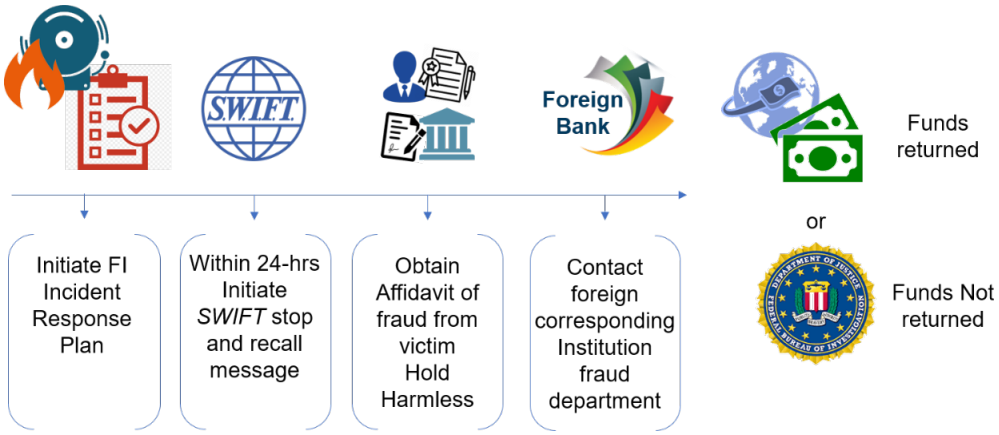

Figure 5: Response workflow for Wire Transfer Incident

Incident Reporting

1. Notify regulator and law enforcement.
2. The FBI and United States Secret Service ("USSS") encourage victims of cybercrime to contact their local FBI[5] or USSS[6] field office and file a complaint online at www.IC3.gov.
3. When reporting, be prepared to provide a general description of this crime, how it occurred, losses experienced, and Wiring/ACH instructions.
4. The FS-ISAC encourages member institutions to report any observed fraudulent activity through the FS-ISAC submission process on the FS-ISAC portal or by contacting the FS- ISAC SOC. Submission through the FS-ISAC portal can be done anonymously and will assist other financial institutions to prevent, detect, and respond to similar attacks and protect their customers.
5. Financial institutions' compliance or anti-money laundering team(s) should submit a Suspicious Activity Report (SAR) utilizing the BEC term to make it easier for law enforcement to track.

[5] http://www.fbi.gov/contact/fo/fo.htm
[6] http://www.secretservice.gov/field_offices.shtml

Conclusion

BEC scams can harm long-standing trusted relationship with bank customers. Understanding the risks, developing educational programs for bank employees and customers, enhancing incident response plans can make a difference.