Payments fraud is on the rise—are you protected?

Payments fraud continues to rise, affecting financial institutions and their clients. Fraudsters have become highly sophisticated, accessing funds of both large and small businesses in the Payments arena. The types of payments fraud also continue to shift year over year. While check fraud is still the most common, wire transfer and ACH fraud are rising significantly.

Payments fraud is as close as your inbox

Fraud attacks take many forms. One of the most common is "phishing" emails. These emails typically contain a clickable link or a place to submit login credentials in order to obtain personal or business information.

Business Email Compromise (BEC) is another common form of payments fraud. And like phishing, BEC is also on the rise and targets businesses of all types and sizes. There are countless variations of this type of fraud, and no individual or company is immune.

What is a Business Email Compromise (BEC)?

A BEC is a digital scam in which fraudsters gain access to business email accounts through various techniques. According to the Association of Financial Professionals (AFP), in 2019 nearly three-fourths of companies reported that they were exposed to business email compromise attacks with more than half of all respondents reporting actual financial losses due to BEC.

Here are two common scenarios of BEC attempts:

Scenario 1
A fraudster gains access to a CEO or CFO email address. A bogus email is sent to an employee in "accounting" requesting a wire transfer to a mule the fraudster controls.

In 2019, the Association for Financial Professionals reported that 81% of companies were victims of actual or attempted payments fraud.
(AFP 2020).

Often times this email will be indicated as "urgent" and/or "confidential," impelling the employee to conduct the transfer quickly and potentially without using the same internal controls they might otherwise practice.

Scenario 2
A fraudster impersonates a trading partner of a company, and sends an email or fax that directs the recipient to change their bank information for all subsequent wire transfers. The request will look nearly identical to a typical request from the trading partner and may even be sent on fraudulent letterhead. Once the changes are made, all subsequent wire transfers to that trading partner, whether legitimate or not, would be sent to the fraudster's bank.

Continued >>

THE LIFECYCLE OF A BUSINESS EMAIL COMPROMISE SCAM*

How criminals can work their way into your email and come away with cash.

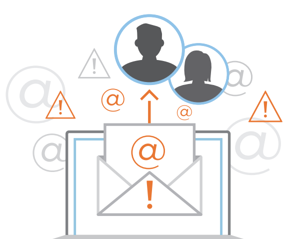
Step 1

FINDING A LIKELY TARGET

Organized crime groups discern and hone in on a susceptible business. They search the internet for exploitable intel on the company and its executives.

Step 2

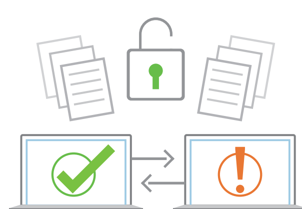
GROOMING



Scammers then focus on a company official (usually in the finance department), testing the waters with phishing emails and/or phone calls. Over a period of days or weeks, they patiently groom and manipulate the contact until they find an opportunity.

Step 3

TAKING THE BAIT



Finally convinced that the offer or opportunity is legitimate, the victim proceeds with the transaction, following the wiring instructions provided by the scammer—and unwittingly opens the door.

Step 4

WIRE TRANSFER

With these funds now in the organized crime group's account, there's a good chance the scammers will go back to their source for more.

*Source: Business E-mail Compromise, Federal Bureau of Investigation, https://www.fbi.gov/news/stories/business-e-mail-compromise-on-the-rise

Same Day ACH

In addition to increased fraud, the payments landscape is moving towards faster settlements across all payment vehicles, including Same Day ACH, which will require businesses to be more diligent than ever.

In September 2017, the National Automated Clearing House Association (NACHA) implemented Same Day ACH, a new rule that allows originators to debit accounts using ACH with settlements no later than the end of the current business day, as opposed to "next day" settlement that ACH has used in the past. While this doesn't mean that your trading partners can now debit your account sooner than is stated in your agreement with them, fraudsters could take this opportunity to initiate same day debits in hopes that accounts are not being actively monitored and/or using an ACH filter or block product.

Now, more than ever, it's vital that companies update internal controls and utilize available fraud prevention products.

At Associated Bank, we take the protection of our clients' funds very seriously, offering sophisticated payable solutions that efficiently support organized and optimized payments.

Mitigating payments fraud

Financial institutions are required to have systems and services in place to safeguard accounts and mitigate risk. They are also required to constantly monitor the threat landscape and improve their information security measures as necessary.

The following checklist offers bank-related risk management processes and procedures to verify that you have the controls in place to protect your organization's finances.

Staff training

- Limit authorization to employees who need it.
- Segregate duties clearly within the accounting department.
- Review system access privileges for all employees regularly, including vendor creation.
- Provide education on phishing and other external dangers.

Internal controls

- Dual authorization procedures should be used for the following transactions: Online ACH, ACH/NACHA/EDI file transmissions, wires and check automation.
- Have policies in place regarding payment requests from "senior management" to protect you from BEC.
- Validate requests from trading partners for changes to payment instructions via callback and/or additional methods.
- Always be suspicious of payment requests that are noted as "urgent" or "confidential" or requested to be handled quietly or quickly.
- Review your accounts on a daily basis to check for unauthorized payments. Depending on the payments network used, there may be recourse if you are a victim.
- As fraudsters often target specific roles within a company, be extremely judicious with what is posted on company websites or social media. Never list titles, job descriptions or other sensitive data if possible.
- Use a "separation of duties" strategy.
- Protect all IDs and passwords.
- Review transactions before they leave the company.
- Conduct surprise audits.
- Never sign checks in advance.
- Implement a system to automatically notify others in authority when sensitive changes are made.
- Review and update signature cards annually.

Continued >>

Security controls

- Review internet security regularly and validate best practices.
- Verify that antivirus controls are adequate.
- Perform daily updates.
- Install software and security patches as they become available.
- Rebuild or replace compromised workstations and devices.
- Use web content filtering.
- Implement a suspicious activity monitoring solution.
- Have a Mobile Device Management (MDM) solution.
- Assess financial institution information security practices.
- Use an offsite backup system for all payment data.

How we can help

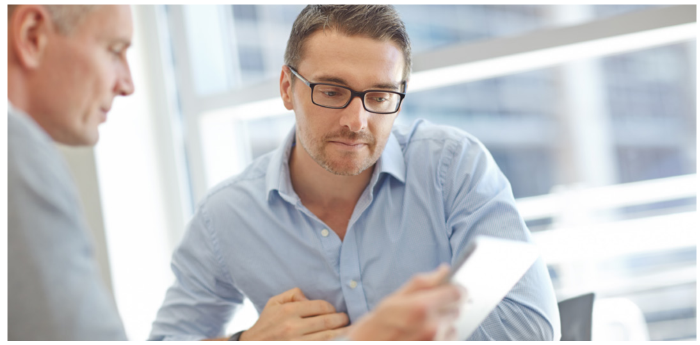
Services to effectively combat fraud include:

ACH Blocks and Filters: The Block service prevents all ACH transactions from posting to your accounts. The Filter service then allows you to review all debits posting to an account, sending those previously authorized to be processed while returning any funds that may have been unauthorized with a single click – one of the most powerful defenses against ACH fraud you can have.

Wire Transfer Fraud Protection: Associated Bank utilizes a number of "behind the scenes" technologies to help keep your accounts safe. Ultimately, however, you need to develop your own controls so that every wire transfer that is initiated has been appropriately authenticated. That includes limiting access to all control elements such as initiation tools, and segregation of initiation and approval roles. Unlike an ACH initiation, settlement of a wire transfer is immediate and there is often no ability to recover funds once a fraudulent wire is sent.

Payee-Positive Pay/Check Fraud Prevention: This service captures payee information with your positive pay check file upload to verify payee in addition to the dollar amount, check number and account number.

Multi-Factor Authentication (MFA): Ensures your accounts and transactions are secure with our enhanced security measures and state-of-the art, layered protection. MFA requirements vary depending on the risk level of your products and services.



Take preventative action

Before your business is faced with fraud, reach out to a relationship manager at your bank and learn about their fraud protection services. Your bank representative will be able to review your current situation and identify opportunities and solutions to protect you against fraud.

To learn more about Associated Bank and the products and services that will protect your accounts, contact your local Associated Bank Relationship Manager or Treasury Management Customer Care Team at 800-270-2707 or TMCC@AssociatedBank.com.

Associated Bank
Your money works here.™

Resources: 2020 AFP Payments Fraud and Control Survey.
Associated Bank, N.A. Member FDIC. (5/20) 16407