CORE BANK

Quarterly Newsletter

ISSUE #08 | Q3 2024

THE FRAUD ISSUE

- The Rising Tide of B2B Payment Fraud
- Business Email Compromise (BEC)
- Payments Fraud
- Corporate Account Takeover (CATO)

THE RISING TIDE OF B2B PAYMENT FRAUD

Business payment fraud is increasingly prevalent, impacting companies of all sizes. According to the 2023 AFP Payments Fraud and Control Survey by JPMorgan, 84% of large businesses and 65% of smaller companies have encountered fraud.

Business email compromise alone led to $2.7 billion in losses in 2022, highlighting the growing sophistication of these attacks.

BUSINESS EMAIL COMPROMISE (BEC)

Staying vigilant is crucial for safeguarding your business against business email compromise attempts and ensuring the security of your sensitive data. Strengthen your defenses by implementing robust verification protocols, providing comprehensive employee training, and enhancing your email security measures.

BEST PRACTICES FOR SAFEGUARDING YOUR BUSINESS:

Verify Email Addresses: Always confirm the legitimacy of email addresses before taking any action.

Delay Financial Transactions: Don't transfer money or sensitive data until you have thoroughly verified the request.

Enable Two-Factor Authentification: Enhance security by using two-factor authentification wherever possible.
Such as: SMS Code or Authenticator Application

Be Cautious Under Pressure: Avoid making hasty decisions when pressured for immediate actions.

Avoid Unsolicited Communications: Steer clear of interacting with unexpected emails, calls, or texts.

"

BUSINESS EMAIL COMPROMISE **ALONE** *led to* **$2.7 BILLION IN LOSSES** *in 2022...*

2022 Federal Bureau of Investigation- Internet Crime Report

CORE BANK

Quarterly Newsletter

ISSUE #08 | Q3 2024

PAYMENTS FRAUD

Last year, payments fraud caused billions of dollars in losses across the United States. Staying ahead of scams exploiting multiple payments rails, from wire to ACH, instant payments and check is a constant challenge –and scams will only become more prevalent as technology advances.

In 2023, $102.6B was lost to payments fraud scams in the Americas.

Source: Nasdaq, 2024 Global Financial Crime

PREVENTING PAYMENT FRAUD: HOW CORE BANK CAN HELP

ACH Positive Pay: Protect your business against fraudulent ACH transactions by using our ACH Positive Pay service, which helps verify transactions before they are processed.

Check Positive Pay: Prevent check fraud with our Check Positive Pay system. This service matches each presented check against a list of issued checks to identify any discrepancies.

Dual Control: Implement dual control procedures to add an extra layer of protection. This means one employee initiates a transaction, and another approves it, reducing the risk of unauthorized transactions.

Tokenization: Use our tokenization service to protect sensitive payment information. Tokenization is required when utilizing ACH and Wire Transfers.

Shift from Paper to Electronic: Shift from traditional paper payments to electronic ones for greater security and efficiency. By transitioning to digital statements, you not only reduce the risk of check fraud but also streamline your payment processes.

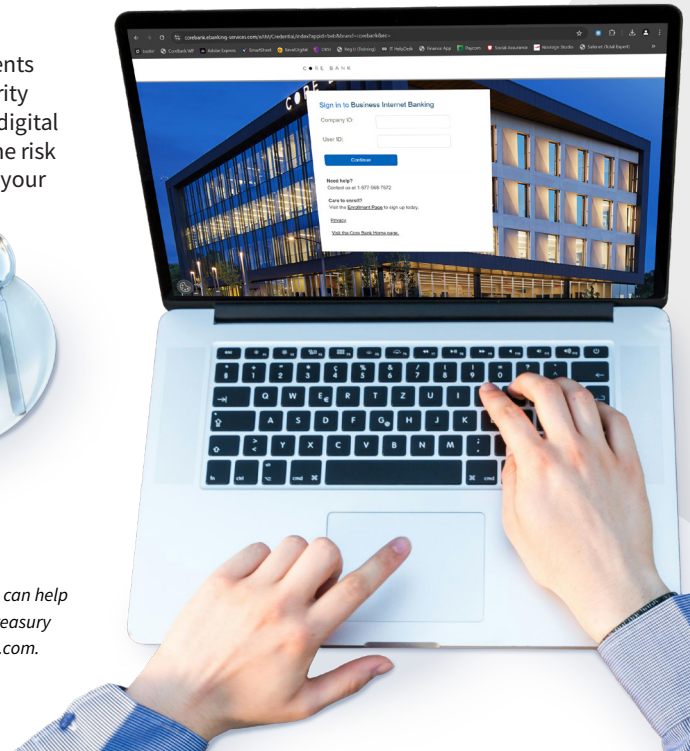
For additional information on how Core Bank can help mitigate payment fraud please contact the Treasury Services Team at treasuryservices@corebank.com.

BEST PRACTICES TO PREVENT CORPORATE ACCOUNT TAKEOVER (CATO):

- **Secure Devices:** Use updated firewalls, anti-malware, and anti-spyware.
- **Avoid Public Wi-Fi:** Conduct financial transactions on secure networks or with a VPN.
- **Separate Devices:** Use different devices for creating and sending wire/ACH instructions.
- **Be Wary Online:** Manually enter URLs and be cautious of suspicious links.
- **Strong Passwords:** Use strong, private passwords and verify any unsolicited requests.

ONGOING MEASURES:

- **Train Employees:** Regularly update security training.
- **Dual Control:** Ensure separate employees handle transaction entry and approval.
- **Monitor Accounts:** Regularly review and reconcile accounts, especially around holidays.



WARNING SIGNS OF A COMPROMISED SYSTEM:

Trouble accessing online banking

Slow computer performance

Unexpected screen changes or reboots

Strange pop-ups or new toolbars

If you notice any of these signs, contact your bank and IT department immediately.