CITY NATIONAL BANK
AN RBC COMPANY

Cyber Security & Fraud Prevention

Trends in the Landscape

Cyber Security Threats are on the rise, as fraudsters employ multiple techniques to compromise employee accounts and then go on to commit fraudulent acts using that access.

Payments Fraud remains a challenge for businesses of all sizes. Over 65% of corporate practitioners reported being targeted by a fraud attack in 2022. Checks remain the most targeted payment method. Corporate/ Commercial Credit Card and electronic payments including ACH targets are rising. Businesses should proactively protect themselves with thorough risk mitigation strategies[1].

While they might look legitimate at first glance, **Phishing Attacks** are designed to harvest sensitive information. Signs that an email link is part of a phishing attack include misspellings, strange message formatting and an email address that doesn't match the sender's purported identity. Never open email attachments or click on links from unknown or suspicious sources, including social media sites. In some instances, links can be the gateway to phishing attacks designed to harvest your information.

With **Social Engineering Fraud** (SEF), fraudsters use information gleaned from social media, overheard conversations, and data breaches to stage conversations with familiarity. Disregard requests that ask you to share your personal or account information unless you are sure the request and requestor are legitimate.

Business Email Compromise (BEC) is designed to spoof or take over a business email account to create, redirect and/or change a transaction, by someone posing as an executive, existing vendor or employee. In 2022, the FBI's Internet Crimes and Complaint Center (IC3) noted potential losses of more than $10.2 billion from criminal cyber activity, with BEC schemes accounting for nearly $2.7 billion[2].

Account Takeover (ATO) uses various methods to change access to an account to remove the actual owner and insert the fraud actor. The goal of this scheme is to compromise the entire account, not just a transaction. Criminals can compromise your account through hacking and change the credentials so you can no longer access or manage it.

Securing Your Finances is Our Top Priority

At City National Bank, we take an aggressive stance against fraud, working closely with you to implement tools and processes to help mitigate risk and protect your bottom line. Your best protection against fraud is caution. Please reach out to your Relationship Manager if you see anything you think may be fraudulent. The City National Bank Fraud Operations Team operates 24 hours a day to support our clients.

Confirm with your Relationship Manager that you are taking advantage of dual control and administration. Dual control for payments and dual administration both provide accountability and an extra layer of protection from account abuse internally, as well as fraud from external parties who might have gained unauthorized access to an account. It requires two different authorized individuals to perform critical actions, where one makes the request for user administration changes and outgoing payments while another individual approves orders.

1. Source: The Association for Financial Professionals (AFP) 2023 Payments Fraud and Control Report
2. Source: IC3 report: https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf

Actions to Help Protect Yourself from Fraud

Your employees are your first line of defense against fraud. Provide training to help them identify fraud and protect your company. Here are some additional steps you can take:

Formalize Your Fraud Approach: Segregate duties and ensure for accounts payable you have more than one person initiating and approving payments.

Minimize Your Digital Footprint: Hackers often use data breaches on a person's inactive social media accounts to gain information that can get them into other important ones. Deactivate your old accounts.

Update All Apps and Devices: Whether it's a smart lightbulb in your home or an app on your phone, consistently updating to the latest version is a key part of staying secure online.

Prevent Attacks from External Media Devices: Disable your computer to "auto-load" removable media (e.g., USB drives, SD cards) and scan these items before you open them.

Lock Your Mobile Devices: Password-protect them to protect against unauthorized use. Only download apps from legitimate online stores.

Change Your Passwords: Use strong passwords and change them frequently. Never share your login information with other people.

Use a Password Manager: Password managers can create strong passwords on your behalf and store them securely -- so you won't have to struggle to remember how to access all of your online accounts.

Use Multi-Factor Authentication: Sometimes called two-factor authentication, this security setting uses a secondary piece of information -- often a code generated by an app or sent to your phone – with your password to make it more difficult for someone to access your account. Authentication tokens can be soft (on your mobile device) or generated on a physical token device.

Validate Requests: Establish internal controls and processes to validate new requests or changes to payment information.

Safeguard Checks and Account Information: Only order secure checks from reputable sources. Keep them in a secured area and limit the number of employees who are allowed to access them. Immediately deface or destroy voided checks and keep track of the serial numbers for them.

Reconcile Accounts Promptly: Review check images and inform the bank immediately if you detect your signatures are forged.

Digitize Payments and Implement Fraud Protection Solutions. We offer these **Treasury Management Solutions** to help prevent fraud:

- ✓ **Check Positive Pay:** May detect fraud by comparing your issued check numbers and dollar amounts against paid check details. Our payee verify feature offers additional protection by matching payee names.
- ✓ **Account Reconciliation:** Automate steps involved in reconciling deposits and payments. Combined with Positive Pay, it's a powerful tool to help prevent check fraud.
- ✓ **ACH Fraud Protection:** With ACH Positive Pay, Blocks and Filter Authorizations, we can customize a solution to help protect your business from fraudulent ACH transactions.
- ✓ **Stop Payments:** Online access to place, edit and cancel stop payment requests without having to call or visit a branch.
- ✓ **Alerts:** Set up Transaction Activity, Payment, and Fraud email alerts to monitor account activity.

Terms and Conditions Apply. Please see the Treasury Management Disclosure and Agreement in the Deposit Account Disclosures available online at cnb.com/agreement. For more information, please see cnb.com/treasury.