TREASURY MANAGEMENT Solutions

Tips & Advice for Your Business

Rising risk—and how to fight back smarter

There was a time when the security advice you were given by a banker was not to write your personal identification code (PIN) on the back of your debit card. Security is no longer that simple:

- **Equifax breach: Equifax says cyber attack may have affected 143 MM**
- **Ransomware: Why some victims with backups still pay**
- **Jason's Deli: Hackers dine out on 2 million payment cards**
- **Target offers $10 MM settlement in data breach**

While ACH is efficient and cost-effective, ACH fraud is on the rise. Fraud involving the Automated Clearing House (ACH) Network, which is used to handle direct deposits, bill payments and cash transfers, is becoming a popular way for hackers to take money from unsuspecting victims. One way they are able to perpetrate the fraud is through an Account Takeover. Account Takeover is a type of identity theft in which a criminal entity steals a company or individual's valid online banking credentials. Small to mid-sized businesses remain the primary target of criminals, but any business or individual account holder can fall victim.

Your Business Can Reduce Risk

Account Takeover attacks are usually a stealth operation. These are quietly perpetrated by the introduction of malware or viruses through a simple email, an infected website or through social engineering. Malware or a virus introduced in the computer system may remain undetected for months—sometimes years—as it tracks and stores security credentials, how your business operates and any other sensitive data.

NACHA's (National Automated Clearing House Association) Risk Management Advisory Group has developed the following business practices for companies of all sizes to consider when reviewing and implementing security procedures to mitigate the threat of Account Takeover. While no single security measure alone is likely to be effective in preventing or mitigating all risks associated with Account Takeover, these are sound best practices.

- Install robust anti-virus and security software for all computer workstations and laptops and ensure that such software is automatically patched regularly and remains current.
- Implement multi-layered system security technology. Anti-virus software alone will not protect a business from most threats. Layering security software constructs a multi-level barrier between business' networks and criminals attempting to access such networks.
- Implement security suites so all security options (i.e., firewall, anti-virus, anti-spyware, anti-malware, etc.) work harmoniously to provide superior protection since security programs from multiple companies sometimes do not work well together, often working against each other, which could leave the computers just as vulnerable as if they had no protection.
- Ensure users are educated around keeping the company's data secure, are knowledgeable and alert to ways in which hackers can access your system.

Online Safety Recommendations:

GENERAL GUIDELINES

- If possible, create a secure financial environment by dedicating one computer exclusively for online banking and cash management activity. This computer should not be connected to the business network, have email capability, or connect to the Internet for any purpose other than online banking.
- If it is not possible to dedicate one computer to banking activity only, don't allow a workstation used for online banking to be used for general web browsing and social networking.
- Verify use of a secure session ("https") in the browser for all online banking.
- Disallow the conduct of online banking activities from public Wi-Fi hot spots like airports, restaurants and shopping centers.
- Cease all online banking activity if the online banking application looks different than usual. Do not continue—and contact Red River Bank immediately.
- Make ACH payment/information forms available only via secure means.

A Quarterly Newsletter from
Red River Bank Treasury Management

Alexandria | Baton Rouge | Shreveport | Lake Charles

RED RIVER BANK
Made in Louisiana. Made for Louisiana.

WEBSITES

It is recommended that a business block access to unnecessary or high-risk websites. At a minimum, a business should prevent access to websites that employees should not visit during work hours. Common sites that carry a high-risk are adult entertainment, online gaming, and personal email.

USER ACCOUNTS

It is recommended that a business:

• Establish user accounts for every computer and limit administrative rights. Employ user settings to avoid accidentally downloading a credential-stealing program. Many small and mid-sized businesses allow all employees to be the network administrator of their computer. Most malware requires the user to be logged in as the network administrator for the malicious program to download.

• Require all employees use strong passwords and change their passwords frequently on both the computer and online banking access.

• Do not allow employees to share passwords.

• Promptly deactivate or remove access rights from employees that no longer require access (e.g., inactive, transferred or terminated employees).

• Take full advantage of options offered by financial institutions to reduce the risk of a large payment being initiated fraudulently. Red River Bank allows customers to set a "user limit" for ACH and wire transfer initiation.

• If possible, institute a dual control process for all internet banking, wire, external transfers and ACH transactions. Having one person initiate the transaction, another approve it and another release the transaction will greatly reduce risk.

visit redriverbank.net

Red River Bank Offers Protection

We are constantly updating our anti-fraud measures to offer you the latest:

• Positive Pay, Partial Positive Pay and ACH Positive Pay to assist clients in protecting their accounts.

  ◦ Positive Pay: Ensures checks presented match the criteria you provide to us.

  ◦ Partial Positive Pay: Allows you to review all checks presented the night before and make pay/return decisions

  ◦ ACH Positive Pay: If the transaction does not meet your requirements it will be returned.

• 128 bit encryption, which is a data/file encryption technique that uses a 128 bit key to encrypt and decrypt data or files.

• SecurLock, which provides clients the ability to lock debit cards, select geographic locations where the card can be used, set merchant locations, transaction spending limits, transaction alerts and review recent transactions.

• Secure authorization code for wire transfers and ACH transactions

• Call-back policy for ACH transactions and wire transfers above a specific dollar amount

Please contact your account officer to ensure you have the protection that is right for you.

Member FDIC