NACHA
The Electronic Payments Association®

Sound Business Practices for Businesses to Mitigate Corporate Account Takeover

This white paper provides sound business practices for companies to implement to safeguard against Corporate Account Takeover. NACHA's Risk Management Advisory Group developed the sound business practices for businesses to consider when reviewing and implementing security procedures to mitigate threats.

Executive Summary

Corporate Account Takeover is a type of business identity theft in which a criminal entity steals a business's valid online banking credentials. Small to mid-sized businesses remain the primary target of criminals, but any business can fall victim to these crimes.

Attacks today are typically perpetrated quietly by the introduction of malware through a simple email or infected website. For a business that has low resistance to such methods of attack, the malware introduced onto its system may remain undetected for weeks or even months. Introducing layered security processes and procedures,technological and otherwise, and other tightened security efforts, can help protect businesses from criminals seeking to drain accounts and steal confidential information. These increased security procedures may help reduce the number of incidents, mitigating financial losses, business risks and reputational damage that can result from such attacks.

NACHA's Risk Management Advisory Group developed the following sound business practices for businesses of all sizes to consider when reviewing and implementing security procedures to mitigate the threat of Corporate Account Takeover. The sound business practices outlined in this paper are not meant to be adopted as exclusive approaches businesses should implement to address risks associated with Corporate Account Takeover, nor are they meant to be considered mandatory . No single security measure alone is likely to be effective in preventing or mitigating all risks associated with Corporate Account Takeover. Similarly, some of these sound business practices may not be appropriate for or applicable to all businesses. Accordingly, each business must identify its own risks and design and implement appropriate security measures to prevent and mitigate risks associated with Corporate Account Takeover.

The sound business practices for businesses outlined in this white paper include:

Computer Security

- Layered System Security
- Online Banking Safety
- Education
- Websites
- User Accounts
- Staying Informed

Account Security

- Dual Control
- Reconcilement
- Account Services
- Reporting Suspicious Activity
- Credentials

Sound Business Practices

Each business should evaluate its risk profile with regard to Corporate Account Takeover and develop and implement a security plan, including sound business practices, to prevent and mitigate risk. Such a plan should consider the unique circumstances of the business. However, in developing the plan, each business should consider the following sound business practices, which are recommended in most cases, and any other identified sound business practices regardless of whether such practices have been communicated by NACHA.

Computer Security

Layered System Security
It is recommended that a business:

- Use appropriate tools to prevent and deter unauthorized access to its network and periodically review such tools to ensure they are up to date. These tools include:
  - o Firewalls
  - o Security suites
  - o Anti-botnet, anti-malware, and anti-spyware programs
  - o Encryption of laptops, hard drives, VPNs or other communication channels
  - o Education of all computer users

- 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 businesses' 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 vendors sometimes do not function well together, often working against each other, which could leave computers as vulnerable as if they had no protection.

Online Banking Safety
It is recommended that a business:

Create a secure financial environment by dedicating one computer exclusively for online banking and cash management activity.

- 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.

• Disallow 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 free Wi-Fi hot spots like airports or Internet cafes.

• Cease all online banking activity if the online banking application appears different and not legitimate. Do not continue and contact the financial institution immediately.

Education

It is recommended that a business:

An employee whose computer becomes infected can infect the entire network. For example, if an employee takes a laptop home and accidentally downloads credential-stealing malware, criminals could gain access to the business's entire network when the employee connects again at work.

• Educate all employees about cybercrimes so they understand that even one infected computer can lead to an account takeover. An employee whose computer becomes infected can infect the entire network. For example, if an employee takes a laptop home and accidentally downloads credential-stealing malware, criminals could gain access to the business's entire network when the employee connects again at work. All employees, even those with no financial responsibilities, should be educated about these threats.

• Always ask, "**Does this email or phone call make sense?**"

o Educate all employees to think critically about each email and phone call received. A business should advise its employees to:

1) Not open suspicious emails or emails from unknown persons. Even opening an email may expose a computer and the network to malware.

2) Ask, "**Does this make sense?**" before taking action in response to an email. If an email is suspicious, do not click on a link or open an attachment. The link could navigate the employee to an infected website or download a malware program. Likewise, attachments and .zip files (compressed files) can contain malware. Employees should be instructed to simply delete the suspicious email and not to click a link or open an attachment. The business can also inquire of a domain lookup service such as "whois.net" or a similar service that allows employees to view the domain registration information of an email sender. If employees do not stop to think and take appropriate action, criminals may be able to lure unsuspecting employees into actions that may infect their computers.

3) Be particularly suspicious of emails or calls purporting to be from a financial institution, government agency or other organization requesting account information, account verification or banking access credentials such as usernames, passwords, Personal Identification Numbers (PINs) and similar information. If such a suspicious email is identified or call is received, the business should call the financial institution to verify

legitimacy. The business should not call the phone number included in the email, click on the link or reply to the sender of such an email.

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 high-risk include adult entertainment, online gaming, social networking and personal email.

• 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 high-risk include adult entertainment, online gaming, social networking and personal email.

User Accounts
It is recommended that a business:

• Establish user accounts for every computer and limit administrative rights. Many malware programs require the user to have network administration privileges to infect the computer.

• Employ "user" settings to avoid unintentionally downloading a credential-stealing program. Many small and mid-sized businesses allow all employees to be the network administrator of their computers. Most malware requires the user to be logged in as the network administrator for the malicious program to download.

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

• Promptly deactivate or remove access rights of employees who 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. Many financial institutions allow customers to set a "user limit" for ACH and wire transfer initiation via their online banking portal.

Staying Informed
It is recommended that a business:

• Stay informed about defenses to Corporate Account Takeover. Since cyber threats change rapidly, it is imperative that all businesses stay informed about evolving threats and adjust security measures in a timely manner. Among other things, this can be achieved by connecting with alert groups, businesses and industry resources about threats and frauds.

Account Security

Dual Control
It is recommended that a business:

- Initiate payments under dual control, with assigned responsibility for transaction origination and authorization. Dual control involves file creation by one employee with file approval and release by another employee on a different computer. Or, require dual use of tokens where a single employee creates a file, but can only release the same file by logging in a second time using a new passcode on the token. Avoid having employees initiate and authorize payment transactions with administrator credentials.

Reconcilement
It is recommended that a business:

- Reconcile accounts online daily; at a minimum, review pending or recently sent ACH files and wire transfers.

Account Services
It is recommended that a business:

- Take advantage of appropriate account services offered by its financial institution. Financial institutions offer a variety of services including positive pay, security tokens, debit blocks, call-backs, etc. Consult your financial institution to identify what security services it offers.

Use multi-factor and multi-channel authentication for business accounts that are permitted to initiate funds transfers. Multi-factor authentication includes at least two of the following: 1) something the person knows (user ID, PIN, password), 2) something the person has (password-generating token, USB token), and 3) something the person owns (biometrics, i.e., fingerprint scan).

- Use multi-factor and multi-channel authentication for business accounts that are permitted to initiate funds transfers. Multi-factor authentication includes at least two of the following: 1) something the person knows (user ID, PIN, password), 2) something the person has (password-generating token, USB token), and 3) something the person owns (biometrics, i.e., fingerprint scan).

Reporting Suspicious Activity
It is recommended that a business:

- Monitor and report suspicious activity. Ongoing monitoring and timely reporting of suspicious activity are crucial to deterring or recovering from these frauds. A business should report anything unusual to the financial institution, such as log-ins at unusual times of day, new user accounts, unauthorized transfers, etc., so the financial institution can immediately block the account and monitor activity.

Credentials
It is recommended that a business:

- Not use administrator credentials issued by its financial institution for day-to-day processing. Criminals use compromised administrator rights to create new users to perpetrate fraud. If criminals gain access to these credentials, they

may set up their own users and profiles on your system to facilitate fraudulent transactions. The criminals can even use the administrator credential to lock legitimate employees out of the system.

Call to Action

This white paper provides sound business practices to help organizations mitigate risk related to Corporate Account Takeover. Businesses should consider these sound business practices, which are recommended in most cases, and any other identified sound business practices, regardless of whether such practices have been communicated by NACHA.

For more information on Corporate Account Takeover and how to mitigate risk, visit NACHA's Corporate Account Takeover Resource Center.