Corporate Account Takeover

Frequently Asked Questions

Why is so much attention being focused on Corporate Account Takeover (CATO)?

Fraud activity continues to increase and evolve, and fraudsters are targeting small to mid-size businesses more frequently than ever before. As your risk increases, it becomes important to educate yourself and your employees on good data security practices in order to prevent your accounts with us and other banks from being compromised. As a bank, we utilize layered data security controls to protect you as best we can, but we need you to also make efforts to protect sensitive information and online account credentials located on your computer systems and devices.

How much does strong data security cost?

The cost, complexity and robustness of data security in based on your business size, the types of information you handle, and the types of online activities you and your staff perform on the business' computer systems. There are some basic measures you can take that won't cost your business anything:

- Enable anti-virus protection and the desktop firewall on all workstations running Windows operating systems.
- Train all of your employees on good data and online security practices, as well as how to recognize fraudulent email and social engineering attempts.
- Utilize the many guides and tips that can be found online. See the list of resources below, or find them on our website.
- Implement password controls, including strong password requirements and changing passwords every 30-60 days.
- Monitor and reconcile all of your banking accounts on a daily basis.
- Verify use of a secure connection (https://) in the browser for all online banking sessions.
- Avoid using automatic login features in browsers and mobile apps.
- Avoid using public wifi connections (at restaurants, hotels, airports, etc.) when accessing sensitive information or online banking accounts.

You can work with your IT staff to determine how to implement strong data security measures at your business.

What if my company doesn't have IT staff?

We understand that many small business either can't afford or do not necessarily need full time IT staff. Many online resources offer free guidance on implementing strong data security practices (see below), and you can also find those resources on our website. You can also contact local IT services providers for technical assistance.

How do I get started?

A data security self-assessment or security risk assessment can help you to determine what risks you face, and can give you direction in developing a data security program.

How can the Bank help?

We provide a data security self-assessment tool and data security resources on our website for you to utilize. We are also here to answer your questions, but as we are not an IT services company, we can't provide you with more than general recommendations and guidance.

What if I'm already compliant with other data security requirements?

If you accept credit and/or debit cards you may already be PCI DSS compliant. If you are a non-consumer ACH originator, you may already be ACH Security Framework compliant. These compliance programs require that certain data security measures are in place, and can be the foundation of a business-wide data security program.

What is PCI-DSS?

The Payment Card Industry Data Security Standard is the standards created and implemented by the PCI Security Council, including Visa, American Express and Discover Card Services. It sets out data security requirements for card merchants, and depth of compliance is based on the type of card processing you perform. See www.pcisecuritystandards.org/security_standards for more detailed information.

What is the ACH Security Framework?

NACHA, the National ACH Association, amended its rules in September 2013 to include data security requirements for both financial institutions and ACH originators to comply with. The requirements include an annual self-assessment, and the development and maintenance of data security policies and procedures.

Online Resources

Websites to Know

- **IC3** | *www.ic3.gov*
- **Your FBI field office** | *www.fbi.gov/contact-us/field/field-offices*
- **Your USSS field office** | *www.secretservice.gov/field_offices.shtml*
- **USSS Electronic Crimes Task Force** | *www.secretservice.gov/ectf.shtml*
- **PCI DSS** | *www.pcisecuritystandards.org/security_standards/pci_dss.shtml*
- **Federal Trade Commission** | *business.ftc.gov*

Learn More About CATO & Data Security

- **IC3** | CATO Fraud Advisory
- **NACHA** | Corporate Account Takeover What You Need to Know
- **NACHA** | Sound Business Practices to Mitigate Corporate Account Takeover
- **Federal Communications Commission** | Small Business Cyber Planner
- **US Chamber of Commerce** | Internet Security Essentials for Business
- **Better Business Bureau** | Data Security Made Simpler
- **National Cyber Security Alliance** | STOP. THINK. CONNECT. Campaign

This document is for informational purposes and is not intended to provide legal advice. The guidance included is not an exhaustive list of actions, and security threats change constantly.