Corporate Account Security Information

Growing Threats to Your Business—Are You Aware?

Corporate Identity Theft (Corporate Account Takeover) is the business equivalent of personal identity theft and occurs when criminal hackers use deceptive social engineering tactics to trick you into performing financial transactions or to install software, often referred to as malware, to control your computer devices, take control over your business email accounts (also known as Business Email Compromise or BEC), and steal your online business credentials. The criminals then use your stolen online business credentials or your business email accounts to initiate fraudulent banking activity.

Your devices can become infected with malware when you attempt to open an infected document attached to an email—or an infected website link within an email. Malware can also be downloaded to a device when you visit a legitimate site, especially a social networking site, and attempt to open a document, video, or photo posted there. Once the malware infects one device, it often has the ability to quickly and efficiently identify and infect other devices within an internal business network—often without detection.

What You Can Do to Protect Yourself and Your Company

Although Pacific Premier Bank uses technologies such as two-factor authentication and encryption methods that help mitigate the risk of fraudulent banking activity, these technologies cannot protect against malware that attack your devices. There are additional controls you should consider implementing to further mitigate the risk of Corporate Account Takeover and fraud.

- Never provide your account information, password, one-time security codes, or token number over the phone, text, or email. We will **never** ask you to enter personal or account information via email, text, or to download an attachment from email, nor ask you for your password, one-time security codes, tokens, or other security credentials via email, text, or phone.
- Initiate ACH and wire transfer payments under dual control, with a transaction originator and a separate transaction authorizer.
- Always verify new wire or ACH instructions using a trusted communication channel. Criminal hackers can pose as a known entity looking to redirect funds to a compromised bank account.
- Employ best practices to secure computer systems. If possible, carry out all online banking activities from a stand-alone, hardened, and completely locked-down computer system from which email and web browsing is not possible. When finished, turn it off or disconnect it from the internet.
- Be suspicious of emails and phone calls claiming to be from a financial institution, government department, or other agency requesting account information, account verification, or banking access credentials such as usernames, passwords, one-time security codes, token codes, and similar information. Opening file attachments or web links in suspicious emails could expose your entire network to malware.
- Install a dedicated, actively managed firewall, especially if your business has a dedicated connection to the internet. A firewall limits the potential for unauthorized access to a network and computers.
- Create strong passwords with at least 12 characters that include a combination of mixed case letters, numbers, and special characters. Use a unique password for each financial institution site that is accessed and change that password regularly. Avoid using dictionary words in your passwords.
- Educate employees on good cybersecurity practices, including how to avoid malware infections on business computers.
- Never access bank, brokerage, or other financial services information using public Wi-Fi at airports, hotels, cafes, libraries, etc. Unauthorized software may have been installed to trap account numbers and sign-on information, leaving you vulnerable to possible fraud. Vulnerabilities in Wi-Fi systems allow an attacker within range of a victim Wi-Fi spot to read information that was previously assumed to be safely encrypted.
- Install commercial antivirus and desktop firewall software on all computer systems. Free software may not provide protection against the latest threats when compared to an industry-standard product. Ensure computers are patched regularly, particularly operating systems, web browsers, and key applications with security patches. It may be possible to sign up for automatic updates for operating systems, browsers, and many applications.

What We Do to Help Mitigate Your Risk

POSITIVE PAY

Pacific Premier Bank offers Positive Pay to help you detect and prevent check fraud.

- Save time by using this automated online tool to review and decision any check that doesn't match your Check Issued list.
- Conveniently upload your Check Issue information through our secure online portal.
- Gain greater control of your cash flow by proactively monitoring all checks that clear your business accounts.

OUT OF BAND AUTHENTICATION

Out of Band provides greater protection from fraudulent access to user account information.

- First-time users logging into their online banking account will be prompted to confirm their identity through the Online Banking Advanced Login Authentication solution, also known as Out of Band.
- Allows users to authenticate using their username and two additional methods—their password and a one-time security code.

MULTI-AUTHENTICATION

Pacific Premier's Business eBanking portal provides a highly secure environment to access your business checking accounts called Multi-Authentication.

- Provides an added layer of security to ensure users have their own unique credentials to access bank information.
- Users are required to log into the online system using the following three items:
  1. Company ID
  2. User ID
  3. Password

DUAL CONTROL ENVIRONMENT

Pacific Premier strongly recommends that our customers operate in a Dual Control environment when initiating ACH and Wire Transfers, as well as Self-Administration tasks. Business eBanking provides our customers with the ability to entitle users with specific privileges such as Initiators and Approvers.

SECURITY TOKENS—OVERVIEW

Online Banking Security Token functionality provides an additional level of encryption security, user validation, and identification.

- During the initiation of Wire Transfers and ACH Batches, the inclusion of RSA SecureID® functionality creates an additional layer of security.
- Approving a Wire Transfer or ACH Transaction requires an eight-digit PIN and a randomly generated token security code (PIN+security code=passcode). The system validates the PIN and security code during the process. If the user does not enter the correct security code or PIN, the system will refuse the attempt.

SUSPICIOUS ACTIVITY

Report unauthorized transactions on your account immediately. You may report the activity in person at any of our branch locations or by calling **855.343.4070**. If you are a victim of internet fraud you should file a complaint at the Internet Crime Complaint Center by visiting **www.ic3.gov**, a partnership between the National White Collar Crime Center and the FBI.

All of us here at Pacific Premier encourage you to reach out to one of our bankers for more information about corporate account security.

Phone: 855.343.4070 **Web:** PPBI.com/cybersecurity

EQUAL HOUSING OPPORTUNITY

Member FDIC

PPB109-CS

PACIFIC PREMIER BANK®