PILGRIM BANK

# SECURITY BEST PRACTICES TO REDUCE RISK OF IDENTITY THEFT FOR COMMERICAL CUSTOMERS

The vast majority of cyber thefts begin with the thieves compromising the computer(s) of business account holders. Perpetrators often monitor the customer's email messages and other activities for days or weeks prior to committing the crime. A business customer is most vulnerable just before a holiday when key employees are on vacation. Another risk period is on a day the business office is relocating or installing new computer equipment. Employees may be distracted and think a problem conducting online banking is due to a new network or equipment. Therefore it is important and necessary for the business customer's employees to follow established security practices.

Basic practices to consider implementing include:

- Provide continuous communication and education to employees using online banking systems. Providing enhanced security awareness training will help ensure employees understand the security risks related to their duties.
- Update anti-virus and anti-malware programs frequently.
- Update, on a regular basis, all computer software to protect against new security vulnerabilities (patch management practices).
- Adhere to dual control procedures.
- Communicate to employees that Passcodes should be strong and should not be stored on the device used to access online banking.
- Transmit wire transfer and ACH instructions via a dedicated and isolated device.
- Practice ongoing account monitoring and reconciliation, especially near the end of the day.
- Adopt advanced security measures by working with consultants or dedicated IT staff.
- Utilize resources provided by trade organizations and agencies that specialize in helping small businesses. See the end of this document for a list of resources.

## PILGRIM BANK RECOMMENDS ALL BUSINESS CUSTOMERS…

- Discourage employees from using public internet access points (such as open access airports, internet cafes, etc.) when accessing business information or accounts.
- Instruct each person to whom you assign an Access ID and Passcode that he or she is not to disclose them to any unauthorized person.
- Communicate to employees that Passcodes should be strong and should not be stored on the device used to access online banking.
- Encrypt sensitive folders.
- Use two separate computers to initiate ACH and Wire Transfer payments.
- Set-up texting, call backs, batch limits, and dual authorization of ACH and Wire Transfer payments.
- Provide continuous communication and education to employees using online banking systems. Providing enhanced security awareness training will help ensure employees understand the security risks related to their duties.
- Update anti-virus and anti-malware programs frequently.
- Update, on a regular basis, all computer software to protect against new security vulnerabilities (patch management practices).

- Adhere to dual control procedures.
- Transmit wire transfer and ACH instructions via a dedicated and isolated device.
- Practice ongoing account monitoring and reconciliation, especially near the end of the day.
- Adopt advanced security measures by working with consultants or dedicated IT staff.
- Utilize resources provided by trade organizations and agencies that specialize in helping small businesses. See the end of this document for a list of resources.
- Consider password protecting or encrypting your smartphone or tablet and having the capability of wiping stored data remotely.

## EXAMPLES OF DECEPTIVE WAYS CRIMINALS CONTACT ACCOUNT HOLDERS

- The FDIC does **not** directly contact bank customers (especially related to ACH and Wire transactions, account suspension, or security alerts), nor does the FDIC request bank customers to install software upgrades. Such messages should be treated as fraudulent and the account holder should permanently delete them and not click on any links.

- Messages or inquiries from the Internal Revenue Service, Better Business Bureau, NACHA, and almost any other organization asking the customer to install software, provide account information or access credentials is probably fraudulent and should be verified before any files are opened, software is installed, or information is provided.

- Phone calls and text messages requesting sensitive information are likely fraudulent. If in doubt, account holders should contact the organization at the phone number the customer obtained from a different source (such as the number they have on file, that is on their most recent statement, or that is from the organization's website). Account holders should not call phone numbers (even with local prefixes) that are listed in the suspicious email or text message.

## WARNING SIGNS THAT YOUR SYSTEM / NETWORK MAY BE COMPROMISED

- Inability to log into online banking (thieves could be blocking customer access so the customer won't see the theft until the criminals have control of the money).
- Dramatic loss of computer speed.
- Changes in the way things appear on the screen.
- Computer locks up so the user is unable to perform any functions.
- Unexpected rebooting or restarting of the computer.
- Unexpected request for a one time password (or token) in the middle of an online session.
- Unusual pop-up messages, especially a message in the middle of a session that says the connection to the bank system is not working (system unavailable, down for maintenance, etc.).
- New or unexpected toolbars and/or icons.
- Inability to shut down or restart the computer.

## INCIDENT RESPONSE PLAN

Since each business is unique, customers should write their own incident response plan. A general template would include:

- The direct contact numbers of key bank employees (including after hour numbers);
- Steps the business account holder should consider to limit further unauthorized transactions, such as:
    - Changing passwords;
    - Disconnecting computers used for Internet banking; and
- Requesting a temporary hold on all other transactions until out-of-band confirmations can be made;
- Information the account holder will provide to assist the bank in recovering their money;
- Contacting their insurance carrier; and
- Working with computer forensic specialists and law enforcement to review appropriate equipment.

## INFORMATION SECURITY LAWS AND STANDARDS AFFECTING BUSINESS OWNERS

Although banks are not responsible for ensuring their account holders comply with information security laws, making business owners aware of consequences for non-compliance if the information is breached can reinforce the message that they need to maintain stronger security. Breaches of credit and debit card information from retail businesses are common. Loss of that information or sensitive personal information can create financial and reputational risks for the business.

When providing security awareness education to corporate customers, banks may want to also alert business owners of the need to safeguard their own customers' sensitive information. Texas statutes related to safeguarding customer information include:

1. Chapter 521 of the Texas Business and Commerce Code, which is known as Identity Theft Enforcement and Protection Act, provides that penalties of up to $50,000 may be imposed for violations. See §521.053 Notification Required Following Breach of Security of Computerized Data. http://www.statutes.legis.state.tx.us/Docs/BC/htm/BC.521.htm#521.053; and

2. 2. Chapter 72 of the Texas Business and Commerce Code relates to disposal of business records. This statute addresses paper and electronic records/information, including information stored on photocopy machines and printers. http://www.statutes.legis.state.tx.us/Docs/BC/htm/BC.72.htm.

The Payment Card Industry Security Standards Council was launched in 2006 to manage security standards related to card processing. Any merchant that accepts credit or debit cards for payment is required to secure their data based on the standards developed by the council. The PCI Security Standards Council's website https://www.pcisecuritystandards.org/security_standards/index.php notes that noncompliance may lead to lawsuits, cancelled accounts, and monetary fines. The website provides information for small business compliance.

## CONTACT US IMMEDIATELY IF YOU NOTICE ANYTHING SUSPICIOUS

- Review all accounts regularly to detect unauthorized activity.
- Notify Pilgrim Bank at 877-303-3111 immediately if you suspect that your Access ID or Passcode has become known to any unauthorized person.
- If at any time you have questions regarding security or possible fraud, please contact our customer service representatives at 877-303-3111 or via e-mail at customerservice@pilgrimbank.bank.

## ADDITIONAL RESOURCES FOR BUSINESS ACCOUNT HOLDERS

1. The Better Business Bureau's website on Better Business Cybersecurity: https://www.bbb.org/all/cyber-security-resources
2. The Small Business Administration's (SBA) website on Protecting and Securing Customer Information: https://www.sba.gov/business-guide/manage-your-business/strengthen-your-cybersecurity
3. The Federal Trade Commission's (FTC) interactive business guide for protecting data: http://www.ftc.gov/bcp/edu/multimedia/interactive/infosecurity/index.html.
4. Texas Department of Banking's website on Corporate Account Takeover: https://www.dob.texas.gov/banks-trust-companies/corporate-account-takeover