Business Identity Theft Protection Guide

~ Commercial Online Banking Customers should perform a related risk assessment and controls evaluation periodically ~

21 ways to protect your business from fraud and identity theft

Business fraudsters and identity thieves are clever and determined and can quickly take advantage of business owners that do not take certain precautions to protect their business.

The following are some of the proactive actions that you and your employees can take to help prevent criminals using your business's identity information to steal from you or commit fraud in your name.

Protect Your Business Bank Accounts from Fraud

1. Enact security and authentication controls to protect against fraudulent wire transfers and electronic transactions.

- **Internal DDoS** attacks target your business's Internet Service Providers (ISP) to distract the business long enough to impersonate it and gain access to their wire and electronic payment accounts.
- **External DDoS** attacks target bank systems and technical resources with the purpose of distracting them long enough to gain unauthorized remote access to a customer's account and commit fraud through Automated Clearing House (ACH) and wire transfers (account takeover).

Wire transfer and electronic payment fraud are serious threats to businesses. Through spyware and compromised banking credentials, criminals can initiate fraudulent payments and transfers out of the business's bank account. Because these transactions occur quickly, businesses often do not catch the fraud in time and are too late to stop the transfer or recover the funds. Businesses hit by wire transfer fraud regularly suffer significant losses and may only recover some, if any, of the stolen funds.

If your business employs wire transfers, contact The Provident Bank and request double or dual authentication on any wires. That means a wire won't automatically be originated when someone requests it. The bank must take the additional step of obtaining a second authorization from someone at your business -- in writing or in person -- before completing it.

- The Provident Bank suggests that you provide us with information about your regular wire transfer transactions (e.g. amount, day, and time).

If your business *does not* use wire transfers, consider inquiring with your bank if you can filter, limit or block wire transfers altogether.

2. Monitor and reconcile your business accounts daily.

- Sign up for Online Banking.
- Register for e-mail alerts.

Frequent account review and immediate reporting of suspicious or fraudulent transactions can reduce your business's liability and potential fraud loss. Online banking allows you to quickly log in to your bank account and view your business account balance and transactions. The Provident Bank also provides

email alerts regarding your account activity, which can help alert you to suspicious transactions. Through online banking, you can also eliminate mailed paper statements which can further reduce the risk that your business banking information may be stolen or exposed.

3. Think "security" when you access your accounts online.

- Access your online banking and other financial accounts using a computer that maintains regularly updated commercial anti-virus / anti-spyware / internet security software.
- Do not rely on limited versions of security software.
- The computer you use to access your accounts should not used by other persons or for non-business activities, such as email or web surfing.
- Use strong, complex passwords that can't be easily guessed by others; they should be at least 8 characters long, including a combination of upper and lower case letters, special characters and numbers.
- Change your passwords every 60 days and do not use the same passwords for other websites or online accounts.
- Don't log in to your online accounts using public access points or Wi-Fi hotspots, which may be insecure.

4. Be wary of phishing scams.

- Do not respond to suspicious e-mails.
- Do not click on suspicious links.

Phishing email scams are designed to trick you or your employees into revealing confidential personal and business account information (e.g. SSN, employer identification number, taxpayer identification number, account number, username, password, etc.) The IRS, government agencies and legitimate financial institutions never request that you provide or "verify" this information through email communications. If you or your employees receive such an email, notify your bank's fraud department. Do not respond to the email and do not click on any links or open any attachments in the email as doing so can connect you to a fraudulent website and/or cause spyware to be installed on your computer.

5. If you pay by company check, enroll in Positive Pay.

The Provident Bank offers Positive Pay services, which can significantly reduce business check fraud losses. When you write business checks, you provide the bank with a list of check numbers and dollar amounts. The bank compares any checks received for payment against your list. If a check doesn't match, it is identified as an "exception" and is not paid.

6. Keep your business checking account supplies secure.

Check stock, deposit slips, endorsement stamps and all other checking account supplies and records should be kept in a secure location not accessible by unauthorized persons.

Protect Your Business Information and Identifiers

7. Keep all documents containing business information or business identifiers in a safe, secure location not accessible by unauthorized persons.

Be certain to protect and secure hard copy documents that contain business identifiers, account numbers and other sensitive information at all times. Be mindful of all persons that may be able to view or have access to these documents (authorized or not), including clients and customers, visitors, contractors, cleaning crew personnel, etc.

8. Securely shred old or unnecessary documents that contain your business information or business identifiers.

Shred any old or unnecessary documents containing business license numbers, business registrations, EIN / TIN, account numbers, etc. using a cross-cut, confetti cut or diamond cut shredder. You can also employ the services of a secure document destruction company. Any documents waiting to be shredded should be placed in a secure locking receptacle or locked storage room not accessible by unauthorized persons.

Protect and Monitor Your Business Credit Card, Supplier and Trade Accounts

9. Maintain an inventory of accounts and key contact information.

Keep a list of your business accounts, including creditor / financial institution, account number(s), card number(s), etc. for billing and fraud departments in a safe, secure location to minimize the time required to make notifications in the event that fraud is discovered.

10. Carefully review and reconcile account statements as soon as they are received.

Be alert for unusual or suspicious purchases or transactions and promptly contact the creditor if you discover any unrecognized or fraudulent activity, no matter how small. Be aware that a common criminal tactic is to make small purchases on a compromised card, typically $5 to $10, and wait to see if the fraudulent transaction is noticed before making larger purchases.

11. Ask trade and credit references to notify you if they are contacted.

If your business provides or maintains a list of trade or credit references, request each reference to notify you if they are contacted by a third party.

Protect and Regularly Review Your Business Credit File

12. Review your business credit reports.

Though Dun & Bradstreet may be the best recognized source of business verification and business credit reporting, the 3 national credit bureaus (Equifax, Experian, and TransUnion) also provide business credit services. You can obtain copies of your business credit reports from each of these organizations and review them for suspicious activity and to ensure that the information is accurate. These organizations also offer fee-based services to monitor your business credit file and alert you to changes.

Dun & Bradstreet	www.dnb.com	Toll free: 1-800-234-3867
Equifax	www.equifax.com	Toll free: 1-800-525-6285
Experian	www.experian.com	Toll free: 1-888-397-3742
TransUnion	www.transunion.com	Toll free: 1-800-680-7289

13. Keep your business and personal finances separate.

Avoid using your personal credit cards, accounts and lines of credit for business and instead use business cards for business-related expenses and transactions. If a business account is compromised, any personal payment methods (including card or account numbers) associated with that account may also be compromised.

Protect Your Business Computers and Networks

14. Restrict the use of your business computers to only business activities.

Activities such as casual internet surfing, use of social networks (e.g. Facebook, Twitter, LinkedIn), online gaming, downloading programs and file sharing, expose your business computers to viruses and spyware that can jeopardize your business operations, your accounts and the confidential information of your business, customers and employees.

15. Install and use regularly updated anti-virus / anti-spyware / Internet security software.

Be certain to install a program that actively scans and is frequently updated to keep up with new threats.

16. Keep security patches and updates current.

- Operating System (Windows, Mac)
- Browser (Internet Explorer, Safari, Firefox, Chrome)
- Microsoft Office
- Adobe products
- Flash
- Java

It is critically important to regularly check for and install any security updates for your computer's operating system and internet browsers to ensure that you have the latest versions designed to protect against known software vulnerabilities. You should set your system to check for and install important security updates no less than weekly.

17. Install and use a firewall on your business computers or network.

A firewall is a software program or hardware device that monitors and controls external connections to your computer and/or network. Many routers include a built in firewall that helps prevent unauthorized or unwanted external connections. Be certain to change the default administrative password on your router.

18. Secure your business's wireless network.

If your business uses a wireless network and it is not secured (encrypted), others can gain access to your network. Average Wi-Fi signals can extend for a few feet beyond the perimeter of the building. Off-the-shelf wireless network devices typically do not come with their security features activated. You must review the product documentation to learn how to set the security features for your device or call the manufacturer if you need assistance. WPA2 is the most commonly used wireless network encryption standard and is available on most modern wireless network devices. Be certain to change the default administrative password on the wireless router.

Know the Risks and Train Your Employees

19. What you and your employees don't know can hurt your business.

Protecting your business and the sensitive information of your business, customers and employees is the responsibility of everyone in your organization. Properly trained employees are your first line of defense because they understand the risks, know how to protect information and can recognize and stop fraud and information security risks before they impact your business.

Protect Your Business's Online and Public Presence

20. Whois Database and domain privacy services.

- Privately register your domain name

Thieves, scammers and spammers frequently peruse the public Whois database, which provides information regarding the registered owner of an internet domain name (including owner name, key contacts, address, email and telephone number) that can be used in a variety of scams and also for spam email. If your business owns one or more internet domains and/or maintains a website, you might consider opting for a domain registration privacy service which replaces your business information in the Whois database with that of the domain service provider. Your business retains full ownership and control of the domain, but your information is better protected from scammers, spammers and prying eyes.

Protect Your Business from Human Manipulation

21. Beware of Social Engineering.

Social engineering is the art of manipulating people so they give up confidential information.

In a social engineering attack, an attacker uses human interaction (social skills) to obtain or compromise information about an organization or its computer systems. An attacker may seem unassuming and respectable, possibly claiming to be a new employee, repair person or researcher. He or she might even offer credentials to support a false identity. However, by asking questions, the crook may be able to piece together enough information to infiltrate an organization's network.

In order to protect your business against social engineering:

- Do not give up employee names or correct people looking for confidential information.
- Be suspicious of unsolicited phone calls, visits or email messages from individuals asking about employees or other internal information. If an unknown individual claims to be from a legitimate organization, verify his or her identity directly with the company.
- Do not provide personal information or information about your organization, including its structure or networks, unless you are certain of a person's authority to have the information.
- Do not reveal personal or financial information in email and do not respond to email solicitations for this information. This includes following links sent in email.
- Don't send sensitive information over the internet before checking a website's security.
- Pay attention to the URL of a website. Malicious websites may look identical to a legitimate site, but the URL may use a variation in spelling or a different domain
  For example:
  - www.criminal.ebay.com (This is ebay.com)
  - www.ebay.criminal.com (This is criminal.com)
- If you are unsure whether an email request is legitimate, verify it by contacting the company directly. Do not use contact information provided on a website connected to the request; instead, check previous statements for contact information. Information about known phishing attacks is also available online from groups such as the Anti-Phishing Working Group (http://www.antiphishing.org).
- Take advantage of any anti-phishing features offered by your email client and web browser.

What do you do if you think you are a victim?

- If you believe your financial accounts may be compromised, contact the Provident Bank's Customer Contact Center at 1-800-448-7768, Monday through Friday, 8 AM to 7 PM and on Saturday 9 AM to 2 PM.
- If you believe you might have revealed sensitive information about your organization, report it to the appropriate people within the organization, including network administrators. They can be alert for any suspicious or unusual activity.
- Immediately change any passwords you might have revealed. If you used the same password for multiple resources, make sure to change it for each account and do not use that password in the future.
- Consider reporting the attack to the police.
- File a report with the Federal Trade Commission (http://www.ftc.gov/).

Resources

For more information visit:

The Provident Security Center
- http://www.providentnj.com/site/SecurityCenter/Main/Content.aspx

US Cert Website
- http://www.us-cert.gov/home-and-business

APWG: Unifying the Global Response to Cybercrime Website
- http://www.antiphishing.org

Much of this information came from the Business Identity Theft Organization at:
- http://www.businessidtheft.org/