Fraud Mitigation Strategies

Business Customer Checklist

Fifth Third Bank is committed to assisting our clients mitigate the risks associated with online fraudulent activity. The online security landscape is in a constant state of change, and we believe one of the best defenses against fraud is an ongoing working partnership between the bank and our clients.

The checklist below represents many of today's online banking best practices. We strongly recommend that you review and implement the items contained in the check list below. If you have any questions, please contact your Relationship Manager.

- ☐ Protect your computers from malicious programs by using anti-virus and anti-spyware software, as well as a firewall. Keep these programs up to date. If your company has one or more Internet sites, it is recommended that you incorporate intrusion detection and vulnerability management.
- ☐ Ensure that your employees cannot override or circumvent security software.
- ☐ Implement a policy of updating your operating system and security software on all computers, and assign someone the responsibility for seeing that this is done on a regular basis.
- ☐ Turn off and remove services that are not needed on computers. Do any of your employees need to use CDs, DVDs, or USB devices? If not, disable these unprotected conduits into and out of your computer system.
- ☐ Proxy your internet traffic to limit user access to malicious sites and to potentially block malicious software from communicating with a Trojan controller should malware make its way onto one of your company's computers.
- ☐ Make sure employee computer profiles have the least privilege possible. Very few of your employees should need "Administrator access."
- ☐ If you have employees who use laptops, consider implementing software that will determine if mobile devices have been infected before allowing them back onto your network.
- ☐ Review your account balance online on a daily basis to identify fraudulent transactions as soon as possible.
- ☐ Use a mail service that blocks or removes email file attachments that are commonly used to spread viruses, such as files that end in .VBS, .BAT, .EXE, .PIF, or .SCR.

FIFTH THIRD BANK

- [ ] Install a pop-up blocker on your system.
- [ ] Establish a procedure that can be used by any employee if they think their computer may be infected. Make sure employees understand this procedure and the importance of using it.
- [ ] Ensure that only approved company applications are deployed on your computers and be sure to keep them updated (patched).
- [ ] Set rules about employee use of the Internet.
- [ ] Never enter personal or customer-specific information (e.g., account numbers, social security numbers, passwords, user IDs, other login credentials, etc.) into a public computer (those located in hotels, airports, libraries, etc.).
- [ ] Make sure all employees use good security habits. Develop a security awareness program that addresses the risks specific to your business and/or to the specific functions within your company. Update it to include any new risks that have developed and review it with your employees on a regular basis.
- [ ] Fifth Third Bank strongly encourages our business customers to download the free Trusteer Rapport software available on our site. This plug-in application is designed to detect malware intrusions and then provide protection to the computer's browser, thus preserving sensitive information. Rapport works with your antivirus and firewall software, and is not designed to replace these valuable tools, but to work with them to provide another layer of security.

A CHECKLIST FOR YOUR FINANCIAL INSTITUTION

In an effort to prevent fraud, it's important to make sure that any financial institution you choose to do business with has the following:

- [ ] **Network Defense-in-Depth –** Financial Institutions should implement a best practice, layered Defense-in-Depth to their network and system infrastructure. This Defense-in-Depth should include both technical and procedural controls.
- [ ] **Strong Authentication –** Financial Institutions should review the Federal Financial Institutions Examination Council's (FFIEC's) guidance, Authentication in an Internet Banking Environment (FIL-103-2005).
- [ ] **Anomalous/Fraudulent Transaction Detection –** Financial Institutions should implement appropriate fraud detection and mitigation best practices that monitors user access behavior and alerts customers to activity that deviates significantly from their normal online banking activity, such as unusually high transaction values.
- [ ] **Out-of-Band Transaction Authentication –** Financial Institutions should consider using manual or transaction authentication systems in concert with fraud detection.

FIFTH THIRD BANK