Business Customer Checklist

While Fifth Third can help ensure the security of your accounts, you play a vital role in preventing and reporting unauthorized account activity. The computer security landscape has changed greatly and there are a number of steps you must take to protect your business from the ever increasing number of threats.

The Fifth Third Bank team is committed to protecting our clients' confidential information but our clients must also play an active role in this effort.

- ☐ 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.
- ☐ 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.
- ☐ Make sure employee computer profiles have the least privilege possible. Very few of your employees should need "Administrator access."
- ☐ 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, PDF, or .SCR.
- ☐ 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).
- ☐ Scan emails.
- ☐ Use an up-to-date browser and apply all patches.
- ☐ 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.

- ☐ Consider adhering to a recent FBI alert that suggests small businesses may want to dedicate one computer, which is never used for reading email or surfing the web, to handle all online banking activity. Having a dedicated computer would reduce the chance of the computer being infected with malware.
- ☐ 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. Conventional security software blocks known attacks, but may not keep up with sophisticated new ones.

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.