Retail Customer Checklist

In addition to the safeguards Fifth Third has put into place, being an educated consumer is your best defense. Here is a checklist of items that will help you to know what to look for and what you can do, which in turn will help you protect your information both on and offline.

Know What To Look For

- ☐ Beware of fraudulent emails or websites known as “phishing” or “web spoofing” that appear to be from Fifth Third or other legitimate sites. Always go directly to Fifth Third’s website by typing “www.53.com” directly into the browser address bar. Never click on unverified links in emails, in pop-up ads, or on other unknown sites. These emails and links may ask for personal information or redirect you to illegitimate sites that look like Fifth Third’s site or appear to have the Fifth Third URL address in the browser address bar.
- ☐ Be cautious about opening email attachments from unknown parties or downloading files from unverified locations. Many of these files contain spyware or key-logging programs that can send information back to a malicious site.
- ☐ Beware of using non-encrypted wireless connections with computers, phones, and portable devices to send sensitive information from public wireless locations or even from home wireless networks. Using scanning devices, individuals can intercept unencrypted signals and view or obtain your information.
- ☐ Beware of “shoulder surfers” while using a computer in public areas who may be trying to intercept your passwords or information.
- ☐ If regular bills or statements stop reaching you, take action. Call the company's customer service number (Fifth Third Customer Service is 1-800-972-3030). Someone may have filed a change-of-address form to divert your mail.
- ☐ Beware of incoming phone calls from “imposters” that who ask you to disclose information by pretending to be fraud investigators or customer service agents calling with an urgent problem about your account. One fraud involves imposters asking only for the three-digit code on the back of your credit card to “verify” possession. When in doubt as to a caller’s identity, always ask to call back at what you know to be a valid customer service number. Review your credit report periodically.

What Can I Do?

- ☐ Maintain and run updated virus, firewall, browser, spyware, and security software on your computer. Review your Internet and email software’s security settings.
- ☐ Use strong passwords with a combination of uppercase and lowercase letters, numbers, and symbols. Change passwords periodically, and always change pre-assigned temporary passwords. When creating PINs and passwords, do not use birth dates, addresses, telephone numbers, etc. that are easily guessed from personal information.
- ☐ Never use the “save ID and password” option in your browser at home, or on a laptop or

public computer.

- ☐ Do not email personal and financial information to non-secure sites. Because of the potential for loss, avoid storing personal information on a laptop computer.
- ☐ Properly dispose of old computers and ensure all sensitive information is removed from the hard drive. Reformatting the hard drive may not be sufficient — use specialized software to erase information.
- ☐ Don't give out financial or personal information online or on the telephone unless you initiated the contact and know the party with whom you're dealing.
- ☐ Safeguard ATM, credit and debit cards—only carry cards you use. Report lost or stolen cards or checks immediately.
- ☐ Memorize personal identification numbers (PINs) and passwords. Never write them on access cards or store them where they can easily be found, such as in wallets, purses, and desks or on computers.
- ☐ Use a crosscut shredder to destroy unnecessary financial documents, including old bank statements, invoices and unwanted pre-approved credit and other financial offers.
- ☐ Review account statements promptly and match credit card receipts. Don't ignore suspicious charges. If questionable or unauthorized charges appear on your bills or statements, call immediately to resolve the discrepancy.
- ☐ Keep personal information off your checks. Never preprint your driver's license or Social Security number on your checks. Remove your Social Security number from your driver's license.
- ☐ Secure personal information in your home, especially if you employ outside help, have roommates, or are having work done in your home.
- ☐ Carry only the minimum amount of identifying information and credit cards in your purse or wallet. Keep your purse or wallet in a safe place at work.
- ☐ Do not leave bill payments in your mailbox if you have the type of mailbox with a flag to signal the box contains mail. Deposit them at your post office or use a post office collection box. Promptly remove incoming mail. If you are going to be away from home, notify your post office and ask them to hold your mail until you return.
- ☐ Order copies of your credit report from each of the three credit bureaus once a year to ensure they are accurate.
- ☐ If you prefer not to receive pre-approved offers of credit, you can opt out of such offers by calling (888) 5OPT OUT. Note: You will be asked to provide your Social Security number to allow consumer reporting agencies to match you to the correct file.
- ☐ Place passwords on your credit card, bank and telephone accounts. Avoid using easily identifiable information like the last four digits of your Social Security number, your telephone number, consecutive numbers, or your mother's maiden name.

For additional information about account fraud and identity theft, you can visit this website:

Federal Trade Commission: www.consumer.gov/idtheft/