Guide to Information Security for Customers of First National Bank of Hereford

INTRODUCTION

We at First National Bank of Hereford are very concerned and proactive in keeping all customer information as secure as possible. In keeping this information secure, we need your help as a customer, to recognize possible breaches to your information. As a bank there are certain situations that are beyond our control to secure. We hope the following guidelines will help you make good decisions with your personal information and how to handle situations that may compromise that information. Just remember to use common sense when dealing with people on the phone or by computer. We at First National Bank of Hereford will never call you and ask for account numbers, social security numbers, passwords, or any other confidential information. As always, if you have any questions please feel free to call us.

IDENTITY THEFT

Identity theft is one of the fastest growing white-collar crimes in the U.S. Identity theft is the fraudulent use of an individual's personal identifying information. Often, identity thieves will use another individual's personal information such as name, social security number, driver's license number, mother's maiden name, date of birth or account number, to fraudulently open new credit card accounts, charge existing credit card accounts, write checks, open bank accounts or obtain new loans.

Identity thieves use various techniques to steal the information. The following are examples of the most common techniques:

- Impersonating victims in order to obtain information from you and other businesses;
- Stealing wallets that contain personal identification information and credit cards;
- Stealing bank statements from the mail;
- Diverting mail from its intended recipients by submitting a change of address form;
- Rummaging through trash for personal data;
- Stealing personal identification information from workplace records; or,
- Intercepting or otherwise obtaining information transmitted electronically.

Identity theft may go undetected for months or even years. Victims of identity theft may not realize that someone has stolen their identity until they are denied credit or until a creditor attempts to collect an unpaid bill. We suggest that you look at your bank statement as soon as it is available each month. This is one of the best ways to prevent fraud.

TYPES OF IDENTITY THEFT

There are two basic types of identity theft: 1) account takeover; and, 2) application fraud.

Account takeover occurs when an identity thief acquires a victim's existing account information and purchases products and services using either the actual credit card/check or the account number and expiration date. Account takeover also includes someone accessing your online banking and bill pay if you have it enabled. Please do the following to secure your accounts:

- Keep user ID and Password secure. If you think your ID or Password has been compromised, please call the bank and we will help you get these reset;
- Keep virus protection and software updates current on your computer;
- Log out of bill pay and online banking when you are not using it;
- When setting up passphrase and answering security questions, use phrases and answers that others will not know;

Application fraud is what is referred to as "true name fraud." With application fraud, the thief uses the victim's social security number and other identifying information to open new accounts in the victim's name – but the phone and/or address information is usually changed to that which is controlled by the thief in order to prevent the victim from learning of the theft and to facilitate the receipt of fraudulent credit cards, etc.

IF YOU ARE A VICTIM OF IDENTITY THEFT

- Contact the fraud departments of each of the three major credit bureaus and request that the credit bureaus place a "fraud alert" and a "victim's statement" in the customer's credit file. The fraud alert puts creditors on notice that the customer has been the victim of fraud and the victim's statement asks creditors not to open additional accounts without first contacting the customer. The following are the phone numbers of the three national credit bureaus:
    - Equifax (800) 525-6285;
    - Experian (888) 397-3742; and,
    - Trans Union (800) 680-7289;
- Request from the credit bureaus a free credit report.
- Review the credit reports in detail to determine if any fraudulent accounts have been established. Determine if any unknown inquiries have been made. Unknown inquiries may be indicators of someone attempting to establish a fraudulent account;
- Contact all financial institutions and creditors where you have accounts. You should request that they restrict access to your account, change any password or close the account altogether, if there is evidence that the account has been the target of identity theft.
- File a police report to document the crime; and,
- Contact the Federal Trade Commission ("FTC") Identity Theft Hotline at (877) ID-THEFT (438-4338). The FTC puts the information into a secure consumer fraud database and shares it with local, state and federal law enforcement agencies. You may also go to the following Web site – www.ftc.gov. These resources can provide you with step-by-step assistance in handling identity theft.

SOCIAL ENGINEERING

Social engineering is the attempt to manipulate or trick a person into providing confidential information to an individual that is not authorized to receive such information. There are four

common types of social engineering techniques: 1) pretext calling; 2) dumpster diving; 3) shoulder surfing; and, 4) identity theft. This section will cover the first three. Identity theft was covered in the prior section.

PRETEXT CALLING

Pretext calling is a fraudulent means of obtaining an individual's personal information. Armed with limited information, such as a person's name, address and/or social security number, a pretext caller may pose as an employee of a business in an attempt to convince you to divulge confidential information.
Information obtained through pretext calling may be sold to debt collection services, attorneys and private investigators for use in court proceedings. Identity thieves may also engage in pretext calling to obtain personal information for use in creating fraudulent accounts.
The list below identifies potential pretext caller situations. While calls that resemble these examples are not necessarily pretext calls, extra care should be taken to ensure the authenticity of the call:

- A caller who cannot provide all relevant information;
- A caller who is abusive and attempts to get information through intimidation;
- A caller who tries to distract you by being overly friendly or engaging you in unrelated "chit-chat" in an effort to change your focus;

DUMPSTER DIVING

Dumpster diving is a common technique used by identity thieves to obtain confidential information. Dumpster diving involves rummaging through your trash to collect your information. Shred or destroy any personal information before disposing of it.

SHOULDER SURFING

Procedures that prevent identity theft and ensure adequate protection of confidential information extend beyond pretext calling and dumpster diving. adequate security procedures also require you to protect against "shoulder surfers."

Shoulder surfers are criminals that acquire personal information through eavesdropping. Shoulder surfers may obtain information while standing in line at a Bank branch, ATM, checkout lines, or watching you as you access information on a computer. Others may use binoculars to spy on their victims. In all instances, the objective is to obtain confidential information.

PASSWORDS

Passwords are unique strings of characters that customers provide in conjunction with a User ID, to gain access to an information resource. Passwords are an important aspect of information security because they are the first line of defense in protecting your information. Passwords are intended to be difficult to guess but still easy to remember. A poorly chosen password may result in the compromise of confidential information that could adversely affect your personal information.

GENERAL PASSWORD GUIDELINES

Everyone uses passwords to access various resources. These resources include access to personal computers, the Internet, accounts, etc. User IDs and passwords are used to authenticate you to the particular resource and are used to track user activity while using that resource.

You must be aware of the characteristics of strong and weak passwords in order to ensure adequate protection of your information. If someone obtains your user ID and password, that individual can imitate you without the system knowing. Any damage created by the intruder will appear to have been created by you.

Poor, weak passwords have the following characteristics:

- The password contains less than eight characters;
- The password is a word found in a dictionary;
- The password is a common usage word such as:

    - Names of family, pets, friends, co-workers, sports, teams, movies, shows, license plate number, birth dates, etc.;
    - Computer terms and names, commands, sites, companies, hardware, software;
    - Birthdays, social security number, User ID and other personal information such as addresses and phone numbers;
    - Word, number or keyboard patterns like “aaabbb,” “qwerty,” “123321;”
    - Repeating patterns like SwC@QE1, SwC@QE2, SwC@QE3, etc.;
    - Any of the above spelled backwards; or,
    - All the same characters or digits, or other commonly used or easily guessed formats.

Strong passwords have the following characteristics:

- Contain both upper and lower case letters;
- Have digits and punctuation characters as well as letters;
- Are at least eight characters long;
- Are not a word in any language, slang, dialect, jargon, etc.; and,
- Are not based on personal information, names of family, etc.

PASSWORD PROTECTION

Refrain from using the same password for Bank accounts as for other non-Bank accounts (i.e., personal email account, etc.). When possible, refrain from using the same password for multiple Bank accounts. Do not share passwords with anyone, including Bank personnel. All passwords must be treated as highly sensitive information.

The following is a list of things that you should NOT do:

- Don’t reveal your password over the phone to anyone;
- Don’t reveal your password in an email message;
- Don’t reveal your password to a Bank employee;
- Don’t talk about your password in front of others;
- Don’t hint at the format of a password (i.e., “my family name”);
- Don’t reveal your password on questionnaires or security forms;

- Don’t share your password with family members;
- Don’t leave your password anywhere on or near your computer (i.e., post-it notes, under mouse pads, etc.);

EMAIL

The use of email creates risks to you that must be properly managed to ensure adequate protection of your information. Risks created through the use of email include:

- Inadequate awareness among email users regarding the fact that email is not a secure form of communication and that privacy and confidentiality is not for certain;
- Links that download virus or malware to your system

SECURITY

Email messages are not secure. Risks to email include someone intercepting the message during transit or the message being inadvertently delivered to the wrong person. Another risk is someone forwarding a private/confidential email to someone else. These risks are increased when email is accessed/delivered through the use of Web mail. As such, you should never include anything in an email message that is private or confidential or that could create the risk of litigation or otherwise put you at risk. The following are some examples of information that should not be included in an email, unless email is sent through a secure site. (ie.https://):

- Passwords;
- Personal information.

OTHER CONSIDERATIONS

INTERNET SECURITY CONCERNS

Viruses and hackers are active on the Internet and try to create and exploit security vulnerabilities. Security services ensuring confidentiality, integrity and authenticity are not automatically provided when using the Internet or Web. In addition, information from Internet sites cannot be relied upon to be authentic or accurate. As such, you must exercise common sense and due care when using the Internet.

SOCIAL MEDIA

The use of social media has become a prevalent form of media in our society. A few forms of this media include but is not limited to: Facebook, Twitter, LinkedIn, etc… Here are some guidelines when using social media:

- Do not put personal information on Social Media sites that you are not willing for everyone to know;
- Any links can contain viruses or malware;
- Putting information on sites that give your location can inform people that you are not at home;
- Anything you post can be traced to the computer that it originates from;

MOBILE BANKING

Mobile banking is the use of a mobile device, commonly a cell phone or tablet computer, to conduct banking activities. These activities can include but are not limited to: balance

inquiry, account alerts, bill payment, and transfer of money between accounts. Following are some risk and guidelines when using your mobile device:

- Virus and Malware can be downloaded to your phone or tablet the same way it is downloaded to your computer. Be careful of any links in emails and websites. This is the predominant way that computers are infected. At this time virus protection options are limited for mobile devices. Stay aware of any new protection that can be added to your device.
- Download apps from reputable stores. Only download from Iphone and Android stores. Downloading from the stores are not 100% safe, but it will help in keeping your device clean from unsafe apps.
- If your phone has the capability of, or can download an app to wipe the system, we recommend that you consider this. This will protect you in case your phone is lost or stolen.
- Password protect phones if possible.

We hope this guidance has been informative and will help you make good decisions when dealing with information security. If you have any questions, please feel free to call us at First National Bank of Hereford. Thanks for being our Partners in Progress.