



## **Protecting Your Personal Information**

### **A. Identity Fraud**

Some key warning signs in recognizing identity fraud include:

- You receive letters from solicitors or debt collectors for debts that aren't yours.
- You receive bills or invoices for goods and services you haven't ordered.
- You are refused a financial service (such as a credit card or a loan) despite having a good credit history.
- You are billed for a mobile phone contract (or similar) set up in your name without your knowledge.

Always remember:

- Lock all valuable documents in a secure place.
- Shred unwanted documents (e.g. old utility bills, credit card receipts etc.)
- Inform all service providers promptly when changing your address.
- Set-up a mail-forwarding arrangement with the post office.
- Never give your personal identification number (PIN) to anyone.
- Check your credit report regularly.

### **B. Bank and Credit Card Statements**

Oftentimes, the early detection or notification of a potential fraudulent situation will prevent the fraudulent act from occurring.

- Regularly check your bank and credit card statements for evidence of fraudulent activity.
- Report suspicious activity to your bank immediately.
- Don't throw out old statements and/or receipts with your household trash. Rather, carefully dispose of these items by shredding them.

### **C. Internet Fraud**

Two common types of online fraud are 'phishing' and 'spyware'. 'Phishing' is a form of online fraud where fake emails or websites, supposedly from a legitimate company, seek to obtain your personal account information. 'Spyware' is software that is downloaded onto your computer without your knowledge. Once there, it can collect information from your system and may transmit it to a third party. Both types of online fraud are done to view and gather your personal information to conduct illegal transactions on your accounts.

If you think you may be a victim of a “phishing” attack:

1. Notify the relevant financial institution.
2. Change your passwords.
3. Contact your local authorities.

Always remember:

- Canyon National Bank or any other financial institution will never send you an email requesting your personal account information.
- Canyon National Bank only requires your security information when logging into your online banking accounts or speaking with a bank representative.
- Do not share your password with anyone.
- Do not open email attachments from people you do not know.
- Be wary of clicking on links as they can lead to false sites.
- Install a reliable anti-spyware application.
- Activate a firewall.
- Be security-conscious when surfing on and downloading from the internet.
- Any unsolicited request for bank account information you receive should be considered fraudulent and reported immediately.

#### **D. Debit/ATM Fraud**

Protecting and safe-keeping your ATM/Debit Card and PIN is the best way you can protect yourself from card fraud.

Always remember:

- Using your PIN to verify transactions will make card fraud considerably more difficult.
- Take care when entering you PIN – always keep it safe, cover the keypad when entering the PIN, never tell anyone or write down your PIN number.
- You should never provide your PIN when making purchases by telephone, via the internet, or by mail.
- Register your Debit Card with **Verified by Visa** to have added security for all your online Visa card purchases. This is a free service developed by Canyon National Bank and Visa with added security features to help ensure that only you use your Visa card to shop online. To register or find out more about the Verified by Visa service just click on the Verified by Visa link on our homepage under the “Helpful Links” area.