Protecting You from Identity Theft

www.StateBankNorthwest.com

Identity Thieves Use A Variety Of Methods To Steal Your Personal Information, Including:

Skimming

Identity thieves steal credit/debit card numbers by using a special storage device when processing your card. Be aware of anything unusual, out of place, or an additional piece of equipment on an ATM or debit card processing machine. Guard your ATM personal Identification Number (PIN) and any ATM or debit card receipts.

Phishing

They pretend to be financial institutions, companies or government agencies, and send email or pop-up messages to get you to reveal your personal information. Don't give out personal information, including your checking account or credit card numbers on the phone, through the mail, or over the Internet unless you know who you are dealing with. Protect your social security number give it out only if absolutely necessary or ask to use another identifier. Never click on links in unsolicited emails.

Hacking

They hack into your email or other online accounts to access your personal information, or into a company's database to access its records. Don't use obvious password like your date of birth, mother's maiden name, or last 4 digits of your social security number. Use firewalls, anti-spyware and anti-virus software to protect your home computer, and keep them up to date.

Old-Fashioned Stealing

Identity Thieves will steal wallets, purses, employer personnel records, and your mail, including bank statements, check orders, and pre-approved credit offers. Keep your personal information in a secure place. Never carry or write your Social Security Number on anything you carry. Don't put outgoing mail in your mailbox, drop it into an official Postal Service collection box. Store checks in a safe place. Rent a Post Office box for additional security. Shred confidential documents.

Regulation E

In general these protections are extended to consumer accounts. Banks follow specific rules for electronic transaction issued by the Federal Reserve Board. Known as Reg E, the rules cover all kinds of situations revolving around transfers made electronically. Under the consumer protections provided under Reg E, consumers can recover internet banking losses according to how soon you detect and report them.

Here is what the Federal rules require: If you report the losses within 2 days of receiving your statement, you can be liable for the first $50. After two days, the amount increases to $500. After 60 days, you could be legally liable for the full amount. These protections can be modified by state law or by policies at your bank, so be sure to ask your banker how these protection apply to your particular situation.

Common Ways To Detect Identity Theft

Detect suspicious activity by routinely monitoring your financial accounts and billing statements.

Be alert to signs that require immediate attention:

Bills that do not arrive as expected
Unexpected credit cards or account statements
Denials of credit for no apparent reason
Calls or letters about purchases you did not make
Charges on your financial statements that you don't recognize

Inspect your credit report

Credit reports contain information about you, including what accounts you have and your bill paying history. You are entitled to give you a free copy of your credit report every 12 months if you ask for it. Visit www.AnnualCreditReport.com or call 1-877-322-8228 to order your free annual credit report. You also can write: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. If you see accounts or addresses you don't recognize or information that is inaccurate, contact the credit reporting company and the information provider. To find out how to correct errors on your credit report, visit ftc.gov/idtheft.

Defend against ID theft as soon as you suspect it

Place a "Fraud Alert" on your credit reports, and review the reports carefully. The alert tells creditors to follow certain procedures before they open new accounts in your name or make changes to your existing accounts. The three nationwide consumer reporting agencies have toll free numbers for placing an initial 90 day fraud alert: a call to one company is sufficient:

Experian: 1-888-397-3742

TransUnion: 1-800-680-7289

Equifax: 1-800-525-6285

Placing a fraud alert entitles you to free copies of your credit reports. Look for inquiries from companies you haven't contacted, accounts you didn't open and debts on your accounts that you can't explain. Contact the security or fraud departments of each company where an account was opened or charged without your okay. Follow up in writing, with copies of supporting documents. Use the ID Theft Affidavit at ftc.gov/idtheft to support your written statement. Ask for verification that the disputed account has been dealt with and the fraudulent debts discharged. Keep copies of documents and records of your conversations about the theft.

File a police report. File a report with law enforcement officials to help you correct your credit report and deal with creditors who may want proof of the crime.

Report the theft to the Federal Trade Commission.

Your report helps law enforcement officials across the country in their investigations.

Online: ftc.gov/idtheft
By phone: 1-877-ID-THEFT (438-4338) or TTY, 1-866-653-4261
By mail: Identity Theft Clearinghouse, Federal Trade Commission, Washington, DC 20580

STATE BANK NORTHWEST

Full Service Banking… on a first basis

SBNW Contact for any questions: Cindy Willman (509) 789-4335
CindyW@StateBankNW.com