Identity Theft Prevention Smart Card

Last Updated: 03/10/2015

Identity Theft Prevention - Do's and Don'ts

- Create unique passwords for each of your accounts to limit the chances of having multiple accounts compromised.
- Keep your computer up-to-date with the latest versions of operating system and anti-virus software protection.
- Never share sensitive information such as credit card or Social Security numbers through text, email, or chats.
- Never use public networks to conduct online financial transactions. Remember to log out of personal accounts opened on public devices.
- Ensure that all communications involving online financial transactions are sent through an SSL encrypted connection ("https://").

Background

Identity theft is currently the fastest growing crime in America. Every year, approximately 9.9 million incidents of identity theft are reported, equating to 19 individuals falling victim every minute. On average, each victim spends 30 to 60 hours and 50 to 500 dollars trying to resolve the issue. While the common conception is that identity thieves are online scammers, new evidence indicates that up to 50% of all reported cases involve theft from a neighbor, co-worker, or family member. Most identity theft cases can be resolved if they are caught early.

Types of Identity Theft and What's at Risk

Identity theft occurs when one individual fraudulently uses another's personal information for financial or personal gain. Though the motives behind identity theft may differ, disseminating sensitive or potentially harmful information places your assets at risk.

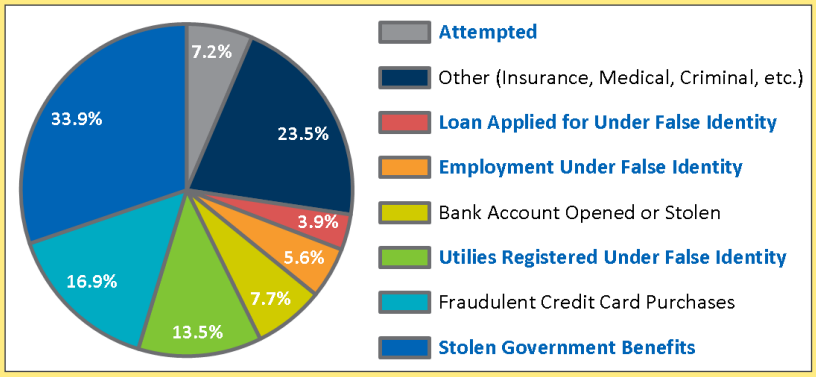
Sensitive Information

- Social Security Number
- Driver's License Number
- Credit Card Number
- Bank Account Number
- Birth Certificate
- Tax Information

Potentially Harmful

- Pets' RFID Numbers
- Utility Account Numbers
- History of Residence
- Unsolicited Credit Offers

What is at Risk?



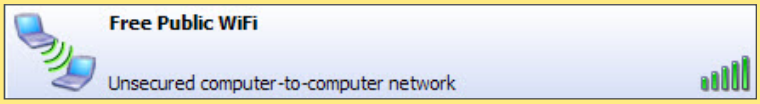
Percentages are according to the Consumer Sentinel Network for total theft reports in 2013. Some reports contained multiple theft types.

ID Theft Types

- Financial
- Insurance
- Medical
- Criminal
- Driver's License
- Social Security
- Synthetic
- Child

Fake Wi-Fi Networks

Fraudsters may establish fake Wi-Fi hotspots to mimic public internet access points. Avoid communicating personal and financial information over public Wi-Fi connections and do not access any unsecured networks.



Social Media Mining

Sharing personal information may allow another individual to apply for a line of credit using your identity or send targeted phishing scams. Avoid sharing home addresses on social profiles and never disclose any of the sensitive information listed above.

Phishing Scams

Phishing scams are among the most popular techniques for acquiring personal information. This information can then be used to open fraudulent accounts or assume control of existing accounts. The model below outlines the common identifiers of a phishing email.

1 **From:** Payment Services <djeib284@swed.edu.is>
Reply-To: <jwdelong1@gmail.com>
Date: Mon, 23 Nov 2014 12:34:13 -0700
2 **Subject:** Suspicious Account Activity!

3 This message is to inform you that your account has exhibited unusual activity within the past 24 hours and has since been locked for security purposes. In order to verify ownership of your account you must respond to this email with the following information:

Name:
Email:
Account Number:
Social Security Number:

5 Failure to verify your account information may result in forfitur of funds.
To see a summary of your account activity, open attached documents or visit out Security Center. 7

4

6

1. Non-descript sender or mismatched email addresses (e.g. "From" and "Reply-To" addresses do not match)
2. Unprofessional subject titles.
3. Phrases demanding the user to share personal information.
4. Absence of a company logo within the email header.
5. Threats to close accounts without compliance or immediate action.
6. Presence of grammatical or spelling errors.
7. Emails containing links to other pages or attachments may contain malicious scripts to install malware.

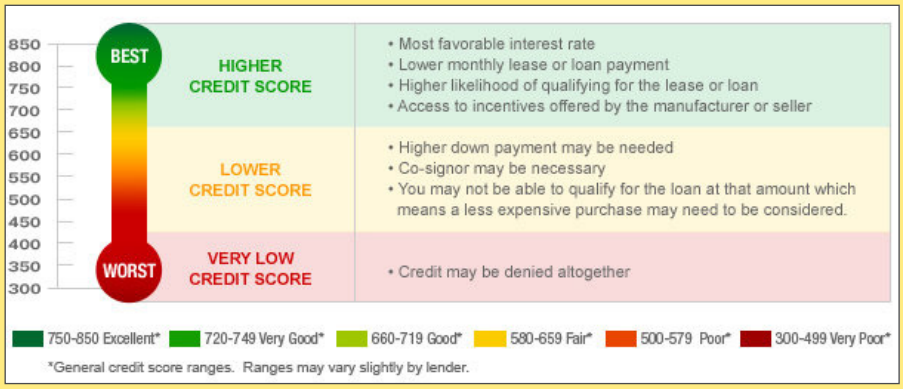
Identity Theft Prevention Smart Card

Last Updated: 03/10/2015

Signs of Identity Theft

Credit scores can be damaged through identity theft. The damages from identity theft can be reduced significantly if caught early. Bank statements should be checked weekly while each of your credit reports should be checked once per year. The following occurrences may indicate a stolen identity:

- Errors appearing on bank and credit card statements.
- Errors appearing on credit reports.
- Financial accounts flagged for suspicious activity.
- Debt collectors call to inform about delinquent debts.
- Problems filing insurance claims.
- Set up fraud alerts on credit cards.



Identity Theft Protection Services

Select companies offer services to monitor customers' credit scores and protect their personal information online. Each company will work with creditors to identify fraudulent activity and restore a customer's reputation. Most packages also offer financial reimbursements for significant personal losses. Individuals should still follow best practice guides to prevent the leak of identity data during online activity.

Identity Protection Service	Data Protection and Recovery Services Offered								
	SSN	Bank Account	Credit Card Numbers	Medical Insurance	Criminal	Driver's License	Computer Security	Financial Coverage	Price per Month
LifeLock	X	X	X		X	X		Up to $1 Million	$22.50
IDENTITY GUARD www.IdentityGuard.com	X	X	X	X	X		X	Up to $1 Million	$14.95
IdentityForce. Protect What Matters Most™	X	X	X	X	X	X	X	Available	$14.99

Resolving Identity Theft

Place an Initial Fraud Alert:
Call one of the three credit report companies listed below and request that an initial fraud alert be placed on your credit scores. The alert lasts for 90 days and prevents any new lines of credit from being opened in your name without a form of verifiable identification. Placing an initial fraud alert entitles you to a free credit report from each of the three credit report companies.

Request Your Credit Scores:
Look for inconsistencies in your credit reports and send letters explaining the misuse to each of the three credit reporting companies. Contact the fraud department of each business that reported a fraudulent transaction on an account in your name.

Create an Identity Theft Report:
File an online complaint with the Federal Trade Commission (FTC) at *www.ftc.gov/complaint* and a police report outlining the details of the theft. Together these documents make up an identity theft report and can be used to remove fraudulent activity from your credit report and obtain information about accounts the identity thief opened or misused.

EQUIFAX®	Experian	TransUnion®
1-800-525-6285	1-888-397-3742	1-800-680-7289

Useful Links - For more information or questions regarding this card email smartcards@novetta.com

Federal Trade Commission	www.consumer.ftc.gov/articles/pdf-0009-taking-charge.pdf
About Money	http://idtheft.about.com/od/identitytheft101/
Protect My ID	www.protectmyid.com/identity-theft-protection-resources
Privacy Right Clearinghouse	www.privacyrights.org/privacy-basics