Preventing Identity Theft

Each year, millions of Americans have their identity stolen. ENG Lending wants you to have the information you need to protect yourself against identity theft. While there are no guarantees about avoiding identity theft, it's important for you to know:

- We will never initiate a request for sensitive information from you (such as, social security number, personal login ID, password, PIN or account number) nor ask you to verify account information via email.

- We strongly suggest that you do not share your personal login ID, password, PIN or account number with anyone, under any circumstances.

If you receive an email that requests this type of action, you should be suspicious of it and contact us immediately at 866-878-2265. We also suggest you report suspicious emails or calls to the Federal Trade Commission through the Internet at www.consumer.gov/idtheft, or by calling 1-877-IDTHEFT.

What is Identity Theft?

Identity theft involves the unlawful acquisition and use of someone's identifying information, such as:

- Name
- Address
- Date of Birth
- Social Security Number
- Mother's Maiden Name
- Driver's License
- Bank or Credit Card Account Number

Thieves then use the information to repeatedly commit fraud in an attempt to duplicate your identity which may include opening new accounts, purchasing automobiles, applying for loans, credit cards, and social security benefits, renting apartments and establishing services with utility and telephone companies. It can have a negative effect on your credit and create a serious financial hassle for you.

How do they get my personal information?

- Lost or stolen personal items: They may obtain your personal information by finding or stealing your checkbooks, credit cards, driver license or Social Security cards.

- Mail: They may steal your mail, including bank and credit card statements, credit card offer, new checks, and tax information. They may also complete a "change of address form" to divert your mail to another location.

- Onlookers: They will watch and/or listen to you conduct personal business such as entering your PIN when you use your ATM or debit card or when you are talking on the telephone.

- Dumpster diving: They may rummage through your trash, the trash of businesses, or public trash dumps in a practice known as "dumpster diving."

- Internet: They use the Internet to look for personal pages that contain information like genealogical data with your mother's maiden name that can be used to set up a credit card account or possibly access existing accounts.

- Phishing: They may obtain personal information from you through the use of "pop-ups" or emails. These emails have Internet links to deceive you into disclosing sensitive information such as bank account numbers and social security numbers. Oftentimes the email appears as if it comes from a trusted source. It directs you to a "spoof" website that encourages you to divulge sensitive information.

- Pretexting: They may obtain your personal information on the phone by posing as a legitimate company and claiming that you have a problem with your account.

- Skimming: They may steal your credit or debit card numbers by capturing the information in a data storage device in a practice known as "skimming." They may swipe your card for an actual purchase, or attach the device to an ATM machine where you may enter or swipe your card.

- Inside Jobs: They get information from businesses or other institutions by:

o stealing records or information while they're on the job

o bribing an employee who has access to these records

o hacking these records

o conning information out of employees

How do I protect my identity?

- Report lost or stolen checks or credit cards immediately.

- Shred all documents containing personal information, like bank statements, unused checks, deposit slips, credit card statements, pay stubs, medical billings, and invoices.

- Don't put your trash out until shortly before it will be picked up.

- Pay bills online or mail bill payments and other items that contain personal information at a U.S. Postal Service drop box rather than in your curb side mailbox. Don't put any mail in your curb side mailbox until shortly before it will be picked up daily.

- Take your mail out of your curb side mailbox as soon as possible after it has been delivered. If you are traveling, have the U.S. Postal Service hold your mail or have someone you trust pick it up daily.

- Limit the information on your checks (for example, don't include driver's license number, social security number, or telephone number), and don't carry around any more cards than necessary.

- Don't give any of your personal information in person, over the telephone, or over the Internet to anyone-unless you have a very good reason to trust them.

- Don't give any of your personal information to any web sites that do not use encryption or other secure methods to protect it.

- Use a firewall if you have a high-speed Internet connection. This software can be purchased on-line or from most software retailers.

- Don't use PINs or other passwords that are easy to guess (for example, don't use birth dates or spouse, child, pet or mother’s maiden names). Regularly change your passwords. Also, create a username that is unique and difficult for others to guess.

- Examine your credit card and financial institution statement immediately upon receipt to determine whether there were any unauthorized transactions. Report any that you find immediately to the financial institution.

- Make a prompt inquiry if bills or statements are not received in a timely fashion-this could mean that they are being diverted by an identity thief.

- Obtain copies of your credit report periodically from each of the three major reporting agencies to be sure that they are accurate. Experian, Equifax, and Trans Union are required to provide you with one free credit report a year.

What do I do if I suspect I'm a victim of fraud or my identity has been stolen?

If you suspect that your personal information has been compromised, follow these important steps:

- Immediately notify us and your other financial institution(s). You'll need to get new account numbers and select a new PIN. If you are in fact a victim of identity theft, we will offer assistance to help remedy the situation.

- Report any suspicious activity immediately. Scrutinize the charges on your financial statements carefully to ensure that they are legitimate. If there is a questionable transaction or a fraudulent transaction, report it right away.

- Call the three major credit bureaus to request that a fraud alert be placed on your credit report.

- Contact your local police department. Financial fraud is a crime.

- Call the Federal Trade Commission's ID Theft hotline at (877) IDTHEFT to report it. The FTC maintains a program to assist victims of identity theft. The Center logs complaints and provides assistance and information to victimized consumers to rectify damage to their credit and personal reputation.

- Notify the U.S. Postal Inspectors Office. Victims of fraud should contact their local post office to report any crime involving stolen mail or use of the mail in furtherance of a fraud scheme. It is a felony.

- Contact the Social Security Administration at (800) 269-0271. The Social Security Hotline allows a victim of identity theft to report misuse of a Social Security number. You may also visit your local Social Security Office to obtain further information.

- Contact the Department of Motor Vehicles. If your driver's license is stolen, report the theft immediately to your local Department of Motor Vehicles. Ensure that a duplicate license was not recently issued in your name to an imposter.

- Keep detailed notes of your repair efforts. Keep a log of all contacts and copies of all documents; follow up your contact calls in writing.

Check these resources for more information on identity theft and what to do it you're a victim:

The Federal Trade Commission (FTC)

The Federal Deposit Insurance Corporation (FDIC)

United States Department of Justice

Equifax

P O Box 105069

Atlanta, GA 30349-5069

www.equifax.com

To order a report: (800) 685-1111

To report fraud: (800) 525-6285

Experian

P O Box 2002

Allen, TX 75013-0949

www.experian.com

To order a report: (888) 397-3742

To report fraud: (888) 397-3742

Trans Union

P O Box 1000

Chester, PA 19022

www.transunion.com

To order a report: (800) 916-8800

To report fraud: (800) 680-7289