Protecting Yourself From Identity Theft And Fake Check Scams

Satellite Conference and Live Webcast
Wednesday, July 16, 2008
2:00 - 4:00 p.m. (Central Time)

Alabama Public Health Training Network

Faculty

Monica S. Sheeler
Consumer Specialist
Office of the Attorney General
State of Alabama

Question

What Three Things Can A Crook Steal From You That Can Totally Ruin Your Life?

- **Name**
- **Date of Birth**
- **Social Security Number**

The Law

Under Alabama Law:
Ala. Code Sec. 19A-8-192

A person commits the crime of identity theft if, without the authorization, consent, or permission of the victim, and with the intent to defraud for his or her own benefit or the benefit of a third person, he or she does any of the following:

The Law

Under Alabama Law:
Ala. Code Sec. 19A-8-192

- **Obtains, records, or accesses identifying information that would assist in accessing financial resources, obtaining identification documents, or obtaining benefits or the victim.**

The Law

Under Alabama Law:
Ala. Code Sec. 19A-8-192

- **Obtains goods or services through the use of identifying information of the victim.**
- **Obtaining identification documents in the victim's name.**

What Is Identifying Information?

Identifying Info Under:
Ala. Code Sec. 13A-8-192(a)(1)

- **Name**
- **Date of Birth**
- **Social Security Number**
- **Credit Card Account Numbers**

What Is Identifying Information?

Identifying Info Under:
Ala. Code Sec. 13A-8-192(a)(1)

- **Bank Account and Debit Card Numbers**
- **Mother's Maiden Name**
- **Passwords to Accounts**
- **Addresses**

Common Types Of Identity Theft

HI-TECH

- **Phising**
- **Skimming**

Common Types Of Identity Theft

LO-TECH

- **Parents/Children/Ex-Spouses**
- **Inside Jobs**
- **Sweepstakes Scams**
- **Housekeepers/Service People**
- **Purse Snatching/Robbery**

Phishing

A Definition

- **The creation and used of a fraudulent but legitimate looking e-mail and website to obtain internet users identification and financial information for criminal purposes.**
- **This is often achieved by using disguised hyperlinks and address bars.**

Pre-Texting A Form Of Phishing

- **Crooks may already have some of your personal information, but need further pieces of information.**
- **Crooks call or email you and pretend to be representatives of your financial institutions or other businesses you interact with.**

Pre-Texting
A Form Of Phishing

- Crooks tell you they need to make sure your account has not been compromised by verifying your security codes, passwords, etc.
- Crooks use this key information to drain your accounts and steal your identity.

Skimming
A Definition

- Illegally obtaining personal information from the swiping of a credit or debit card through a device that reads the card holders name, card number, expiration dates, and an encrypted verification code.

Skimming
A Definition

- The information is normally stored on a device known as a "skimmer" which is then later downloaded into a computer. Skimmer devices can hold up to 500 individual card details.

Low Tech Crooks

- PARENTS/CHILDREN/EX-SPOUSE: can steal the identity of their "Loved" one.
- INSIDE JOBS/SERVICE PEOPLE: appliance repairperson, cable person, pest control, etc.
- SWEEPSTAKES SCAMS: lure you into believing you have one a prize while stealing your identity.

Low Tech Crooks

- HOUSEKEEPERS: dishonest housekeepers may pilferage through your personal items and steal your identity.
- MAILBOX THEFT: crooks see the red flag up signaling them that there is personal info in the box.

Low Tech Crooks

- DUMPSTER DIVING/TRASH BUNNIES: crooks that pilferage through trash dumpsters looking for any type of information on you that they can obtain.

Red Flag Warnings

- Receipt of actual credit approval notifications—not preapprovals.
- Suddenly stop receiving monthly statements.
- Unexplained credit card charges.
- Calls or letters from unknown credit collection agencies.
- New or renewed credit cards not received.

Protecting Against Identity Theft

- Secure your mail.
- Keep telephone conversations private.
- Keep financial information private.
- Be careful when using the internet.
- Protect your Social Security Number.
- Regularly monitor your credit report.

Secure Your Mail

- Pick up your mail daily
- Have mail held by Postal Service when you are out of town.
- Shred mail such as pre-approved credit card offers before throwing away.
- Put outgoing mail in a secure receptacle.
- Cut down on unsolicited offers by calling 1-888-5-OPT-OUT (1-888-567-8688)

Keep Telephone Conversations Private

Know who you are talking to!!!

- Be very careful about giving your personal information out over the phone.
- Be wary of giving your personal information to a person or company that contacts you.

Keep Telephone Conversations Private

Know who you are talking to!!!

- Ask the caller to give you a number you can call to verify his/her identity.
- Ask the caller to send you the information in writing.

Keep Telephone Conversations Private

Know who you are talking to!!!

- To reduce the number of sales calls you receive, register on the national DO NOT CALL list by calling 1-888-382-1222 or going to www.donotcall.gov

Keep Financial Information Private

- Carry only the credit cards you need.
- Be aware of people around you when using cards and/or checks.
- Limit the information printed on your checks.

Keep Financial Information Private

- Store blank checks in a secure place.
- Pick up new checks at the bank.
- Be stingy about giving out account numbers or other financial information to people.

Use The Internet Carefully

- Be very careful about giving out ANY personal information over the internet.
- Never give out personal information over the internet unless you are using a secure website.
- When shopping on-line, if you make a purchase, use a credit card so that you will have the protection of the Fair Credit Billing Act.

Use The Internet Carefully

- To avoid becoming a victim of "Phishing" be suspicious of any emails you did not solicit which urgently request your personal information. The companies you do business with already have that information.

Use The Internet Carefully

- Do not fill out forms over the internet asking for your personal information unless you know for certain that the email is legitimate.

Protect You Social Security Number

- Be VERY cautious about giving out your Social Security Number. If someone asks you for it, ask him/her why the number is needed, what will happen if you do not give out the number, etc.

Protect You Social Security Number

- Do not carry your Social Security card in your wallet. Store it in a safe place, and take it out only when you know that you will need it, such as when starting a new job.

Protect You Social Security Number

- Carefully examine your Social Security earnings statement to make sure no one is using your Social Security number to work.

Regularly Monitor Your Credit Report

- Even if you follow all of these tips, there is no way to completely prevent your identity from being stolen.

Regularly Monitor Your Credit Report

- Often victims of identity theft do not find out that their information has been stolen until they receive a collection notice or they are turned down for a load or job based on poor credit.

Regularly Monitor Your Credit Report

- To keep this from happening to you check your credit report periodically.
- www.annualcreditreport.com or 1-877-322-8228 to obtain your FREE credit report.

What If I Become A Victim? Take Action!!!!!

I. Get a police report and contact the Federal Trade Commission.
II. Contact the three major credit bureaus and have a fraud alert placed on your account.
III. Contact creditors where fraudulent accounts were opened or fraudulent charges were made.

Police Report – Why Should I File One?

- They are the basis for starting a criminal investigation.
- They are needed by identity theft victims to provide some assurance to the creditors that this is a real crime, rather than someone trying to get out of paying.

Police Report – Why Should I File One?

- Creditors often require a copy of the police report for challenged accounts and charges.

Why Should I Contact The Federal Trade Commission?

- Information will be entered into the CONSUMER SENTINEL database and may assist law enforcement in other jurisdictions on related matters.

Why Should I Contact The Federal Trade Commission?

- FTC has great information for Identity Theft Victims on what to do to clear up their credit reports and challenge fraudulent accounts and charges and what legal protects that victims may have.

Why Immediately Contact The Three Major Credit Bureaus?

- Credit bureaus can place "Fraud Alerts" on accounts so that, if anyone tries to open a new credit account, the victim will be notified first.

Why Contact Creditors Immediately And Follow Up In Writing?

- Time is of the essence because many federal protections that limit the victim's financial loss are time-sensitive.

Fake Checks Scams How They Work

- You are contacted by mail, telephone or email.
- You are told that you have won an international lottery prize, or that you have the opportunity to purchase tickets in a foreign lottery.

Fake Checks Scams How They Work

- You are told that you must mail or wire the "taxes" or other payments in order to receive your prize.
- You usually have to deposit the fake check in your account then wire the crooks "taxes" on the money you have "supposedly" won.

Protecting Yourself From Fake Check Scams Tips From The FTC

- Shred any offer that asks you to pay for a prize or a gift. If it's free or a gift you shouldn't have to pay for it. Free is free
- Resist the urge to enter foreign lotteries. It is illegal to play a foreign lottery through the mail or the telephone.
- Know who you are dealing with and never wire money to strangers.

What Should I Do If I Become A Victim Of A Fake Check Scam?

- Report it to your local law enforcement agency.
- The Federal Trade Commission
- The U.S. Postal Inspector
- Your state or local consumer protection agency.

Need To Know Numbers And Websites

Attorney General's Consumer Hotline
1-800-392-5658
www.ago.state.al.us

Federal Trade Commission
1-877-438-4338
www.ftc.gov

Need To Know Numbers And Websites

Annual Credit Report
1-877-322-8228
www.annualcreditreport.com

Equifax
1-800-525-6285
www.equifax.com

Need To Know Numbers And Websites

Experian
1-888-397-3742
www.experian.com

Transunion
1-800-360-7289
www.transunion.com

Office Of Victim's Assistance
Toll free
1-800-626-7676
www.ago.state.al.us/victim

JANETTE GRANTHAM CARR
VICTIM SERVICE OFFICER

DORIS HANCOCK
VICTIM SERVICE OFFICER

VICKIE TODD
ADMINISTRATIVE ASSISTANT

HOW TO CONTACT US

ATTORNEY GENERAL'S CONSUMER PROTECTION HOTLINE
TOLL FREE
1-800-392-5658