Deterring Identity Theft

THE EVOLUTION OF IDENTITY THEFT

Incidences of identity fraud increased in 2012 for the second consecutive year, affecting 5.26% of U.S. adults. This increase was driven by dramatic jumps in the two most severe fraud types: new account fraud (NAF) and account takeover fraud (ATF). – Javelin 2013 Identity Fraud Report: Data Breaches Becoming a Treasure Trove for Fraudsters

- **Identity fraud incidents and amount stolen increased** – The number of identity fraud incidents increased by one million more consumers over the past year, and the dollar amount stolen increased by $21 billion. This equates to 1 incident of identity fraud every 3 seconds.

- **1 in 4 data breach notification recipients became a victim of identity fraud** – The study found consumers who had their Social Security Number compromised in a data breach were 5 times more likely to be a fraud victim than an average consumer.

- **Fraudsters misuse information fewer days than before** – Consumer information was misused for an average of 48 days in 2012, down from 55 days in 2011 and 95 days in 2010.

Someone becomes a victim of identity theft every three seconds. One American in five has already been affected. You or a member of your family could become a victim. This pamphlet can help protect you and members of your family against the damaging effect identity theft crimes can have on the victim.

Identity theft occurs when an individual’s Social Security Number (SSN), credit card account number, driver’s license number, bank account number, or other personal identifier is captured and used to open new accounts, take over existing accounts, apply for loans, initiate services, access government benefits or commit other crimes.

Identity theft has grown along with advancements in computers, scanners, digital copiers, and desktop publishing. There are three easy steps to take to safeguard your personal data:

1. **Disable Java.** Apple no longer ships its computers with Java enabled by default and disabled the software remotely on Mac computers where it had already been installed. Those who do not own Macs can disable the software using detailed instructions on the US Dept of Homeland Security website at [http://www.us-cert.gov/ncas/alerts/TA13-064A](http://www.us-cert.gov/ncas/alerts/TA13-064A)

2. **Observe good password practices.** Use different passwords for different sites and use long passwords with eight or more characters. Include letters, punctuation, symbols, and numbers. To keep strong passwords effective, change them regularly.

3. **Review your credit reports.** Request your free credit report for each member of your family, including children. Scrutinize it to verify all personal and credit information is correct. It’s not just about checking name and address, but also looking for accounts you didn’t open, unexplained charges on valid accounts, unfamiliar addresses and the number of inquiries. Write to each creditor and consumer reporting agency for any identified discrepancies to ensure inaccurate data is removed or corrected.

**Free annual credit reports can be ordered in any of three ways:**

<table>
<thead>
<tr>
<th>By Calling:</th>
<th>By Writing:</th>
<th>Online:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1-877-322-8228</td>
<td>Annual Credit Report Services</td>
<td>annualcreditreport.com</td>
</tr>
<tr>
<td></td>
<td>P.O. Box 105283</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Atlanta, GA 30348-5283</td>
<td></td>
</tr>
</tbody>
</table>
### TIPS FOR DETECTING, PREVENTING, AND MITIGATING IDENTITY THEFT

<table>
<thead>
<tr>
<th>Tip</th>
<th>Tip</th>
</tr>
</thead>
<tbody>
<tr>
<td>Guard against phishing and other online schemes by not opening or responding to suspicious emails</td>
<td>Avoid disclosing personal information to strangers who contact you cold on the phone, in writing, via email or in person</td>
</tr>
<tr>
<td>Invest in firewall/anti-virus software to protect valuable data on your computer</td>
<td>Use caution when accessing sites or downloading software</td>
</tr>
<tr>
<td>Protect your ATM account - do not write your PIN on your card</td>
<td>Protect your driver’s license</td>
</tr>
<tr>
<td>Be careful when you leave your checkbook, wallet, purse, or laptop in an unattended vehicle</td>
<td>Remove unnecessary credit cards and other items from your wallet or purse</td>
</tr>
<tr>
<td>Shred documents containing personal information with a cross shredding machine</td>
<td>Review financial records promptly</td>
</tr>
<tr>
<td>Remove your personal data before donating or selling a used computer either by using an erasing application or destroying the hard drive</td>
<td>Avoid putting payments, completed applications, or any documents with personal information in your mailbox</td>
</tr>
</tbody>
</table>

### IMPORTANT CONTACT INFORMATION

#### Credit Reporting Bureaus:

**Equifax:**
- www.equifax.com
- To report fraud: 1-800-525-6285

**Experian:**
- www.experian.com
- To report fraud: 1-888-397-3742

**TransUnion:**
- www.transunion.com
- To report fraud: 1-800-680-7289

#### Federal Trade Commission:
- www.consumer.gov/section/scams-and-identity-theft
  - Fraud hotline: 1-877-438-4338

#### Social Security Administration:
- www.ssa.gov/
  - Fraud hotline: 1-800-269-0271

### IDENTITY THEFT CONTACT CHECKLIST

To mitigate damage to your credit and good name, the following entities should be notified as soon as an identity theft crime is known or suspected to have occurred:

1. **Local Law Enforcement Agency**
   a. Request that a case be opened
   b. Obtain a copy of the police report

2. **Credit Card Issuer (s)**
   a. ________________________________
   b. ________________________________
   c. ▪ Close accounts where fraud has occurred or may occur
   ▪ Open new accounts with new passwords or PINs

3. **Financial Institutions**
   a. ________________________________
   b. ________________________________
   ▪ Close ATM/Debit accounts where fraud has occurred or may occur
   ▪ Close checking, savings and other accounts where fraud has or may occur
   ▪ Alert recipients to the situation and arrange alternate payment for any valid checks that have been written
   ▪ Open new accounts with new passwords or PINs

4. **Credit Reporting Bureau Fraud Units**
   - Notify one of the three bureaus to request and review a copy of your credit report
   - Initiate a fraud alert or victim’s statement as appropriate

5. **Federal Trade Commission Fraud Hotline**
   ▪ File a report
   ▪ Request a copy of the FTC fraud affidavit

6. **Others (if applicable)**
   ▪ US Postal Inspection Service
   ▪ Social Security Administration
   ▪ State driver’s license bureau
   ▪ US Dept of State Passport Office
   ▪ Internal Revenue Service
   ▪ Stock brokers and mutual fund or retirement account managers
   ▪ Medicare/Medicaid

### Additional Resources

- [www.consumer.ftc.gov/](http://www.consumer.ftc.gov/)
- [En Español www.consumidor.ftc.gov/](http://www.consumidor.ftc.gov/)