

PROTECT YOUR IDENTITY

IDENTITY THEFT NEWSLETTER

Don't become a victim.

JULY 2011 / VOL. 9

How long can the effects of identity theft last?

It's difficult to predict how long the effects of identity theft may linger. That's because it depends on many factors including the type of theft, whether the thief sold or passed your information on to other thieves, whether the thief is caught, and problems related to correcting your credit report.

Victims of identity theft should monitor financial records for several months after they discover the crime. Victims should review their credit reports once every three months in the first year of the theft, and once a year thereafter. Stay alert for other signs of identity theft.

Don't delay in correcting your records and contacting all companies that opened fraudulent accounts. Make the initial contact by phone, even though you will normally need to follow up in writing. The longer the inaccurate information goes uncorrected, the longer it will take to resolve the problem.

Fight identity theft...Take advantage of our safe and secure shredding and recycling service.

Stay tuned for information regarding our next Free Document Shred Day, coming this fall!

COLLEGE BOUND STUDENTS:

Vulnerable as Identity Theft Targets



Students heading to college and young adults living away from their parents' home for the first time are particularly vulnerable to Identity Theft. Below are some tips for College-bound students to fight identity theft:

- 1** School mailboxes can be easily tampered with and are not always safe. Instead of having sensitive (bank, legal, personal) documents sent to your apartment or dorm room, have them sent to a permanent address (your parents' home or the post office) or sent requiring your signature.
- 2** Invest in a fire-proof lock box to store all your important documents. This can be vital when you are sharing a living space and can't control everyone that comes and goes. You should lock up your Social Security card, passport and bank and credit card statements. Shred any important financial documents that come in the mail and never leave any sensitive mail lying out.
- 3** Never answer a friend-in-distress message on email or Facebook. Most likely if a friend is desperate for money, they'll call you directly rather than contact you online - 99% of the time these are Nigerian scams. Also, never click on an unidentified link that a friend has posted. Check to be sure what you are clicking on is not a virus.
- 4** Always check your credit or debit card statements closely for any suspicious activity. The sooner you identify any potential fraud, the less you'll suffer in the long run. Also, always say NO to loaning anyone your credit or debit card. You never know if it will end up in the hands of an Identity Thief.
- 5** Make sure your computer has up-to-date anti-virus and spyware software. Always install any updates and patches to your computer's operating system or browser software. They will help keep your computer safe from any new advances by on-line identity thieves.
- 6** When shopping on unfamiliar websites, always check out the company first. Click on their trust seals to confirm they are legitimate. Make sure they are a secure site encrypted using SSL.
- 7** Check your credit report three times a year with all three reporting bureaus for any suspicious activity or inaccuracies. You can do this at no expense by visiting the website www.annualcreditreport.com. Order your report from just one Credit Bureau the first time and then 4 months later from the second bureau and 4 months after that from the third bureau.

Although no one is completely immune to identity theft, college-bound students are significantly more vulnerable. Following these steps will lower the likeliness that Identity Theft will happen to you or your child.

This newsletter is brought to you by



ChelseaGroton Bank

Member
FDIC

860-448-4100 • 860-823-4800
860-599-2406 • chelseagroton.com



Scan the QR Code to download the PDF version of this newsletter.

IDENTITY THEFT CRIMINALS MAY TARGET U.S. CHILDREN MORE THAN ADULTS

Stolen Social Security numbers for children as young as five months old are being used to secure employment, open credit card and bank accounts, purchase homes and automobiles and obtain driver's licenses. As a result of this new cyber epidemic, children are discovering their credit and credibility are destroyed just as they enter adulthood. As a consequence, they are being denied internships, student loans, and apartments due to attacks on their identity that occurred years earlier. Experts predict the damage to children will get even worse with healthcare identity theft on the rise

Follow these tips to help keep your child's information from getting into the wrong hands.

1. Check for red flags:
 - A parent receives mail in the child's name, especially pre-approved credit offers, a warning sign of an open credit file.
 - A parent tries to open a bank account for the child and finds one already in existence.
2. Teach children about the danger of sharing personal information online and make sure they understand the importance of privacy.
3. Keep your profile on social networking sites free of private information, like your address, family member names, and date of birth. Make sure your children are doing the same by regularly monitoring their profiles. Make sure all of the privacy settings on social networking sites are set so that your profile can only be viewed by friends and family, not the general public.
4. Make sure anti-virus software and spyware is installed on your computer, and monitor your child's internet usage and e-mails.
5. Protect personal information by keeping it in a safe place where others can't get to it.
6. Resist giving out your child's Social Security number unless absolutely required. This includes to schools, which can sometimes use an alternate set of digits to identify your child. Places like the local recreation center, summer camps, and other organizations do not need your child's SSN. Leave the SSN field blank on forms, and only supply it if the organization follows up.
7. If a relative asks for your child's personal information to set up a monetary gift fund in their name, ask for documentation of the account before handing over the SSN and other required info.
8. Don't carry your child's Social Security card or number with you. Keep it locked up, and only access it when you need it.
9. Shred any document that you no longer need that contains your child's private information.
10. Check your child's credit every few years. Children under 13 years of age shouldn't have a credit report in their name, so ideally there won't be anything to check.

How to Get Your Child's Credit Report

It's a good idea to check your child's credit report every few years for signs of identity theft. To do this, you must contact each of the three credit bureaus – Experian, Equifax, and TransUnion – in writing. (If your child is under 13 years of age, you cannot access his or her credit report online due to the Children's Online Privacy Protection Act.)

Send the letter via certified mail, return receipt requested. Make a note of the date you sent the letter, and when you received a response. You'll need to include documentation that proves you are the parent, such as a photocopy of a driver's license.

The credit bureaus do not knowingly keep credit reports on persons younger than 13 years old. The best case scenario when you request your minor's credit report is to be told by the bureaus that they have nothing on file for your child.

Your child can request his or her own credit report online if they are at least 14 years of age. For bureau-specific instructions, visit each of the agency's websites. Since each bureau holds different information, it's important to get credit reports from all three bureaus for the most comprehensive scan of your child's credit. Request a free credit report online at

www.annualcreditreport.com.

TransUnion:

1-800-680-7289
P.O. Box 6790
Fullerton, California 92834-6790
transunion.com

Equifax:

1-800-525-6285
P.O. Box 740241
Atlanta, Georgia 30374-0241
equifax.com

Experian:

1-888-EXPERIAN (397-3742)
P.O. Box 9554
Allen, Texas 75013
experian.com

TIPS TO STAY SAFE ON SOCIAL-NETWORKING SITES:

- Never post your exact date and place of birth. It's invaluable information to identity thieves, particularly when the two are bundled together.
- Never post your address, phone number or email address. This is plum information to scammers and marketers who are looking for nuggets of your identity.
- Control who can see your personal information. Many social-networking sites have privacy features, but they change often. Know what they are, stay on top of them and restrict your page to your real friends, not friends of friends or someone you met in a bar.
- Limit information about your activities. If you must brag about a trip or a fabulous party, do it after the fact. Announcing that you are going to be away from home is an invitation to have your home burglarized.
- Remember that what you post is public and permanent. Don't put up embarrassing photos that you wouldn't show your grandmother. Don't complain about your job or your boss. Don't say something to or about someone that you wouldn't say to his face. Don't threaten others.
- Know the four types of Facebook users: friends, outsiders, businesses and enemies.
- You should know exactly who wants to be your friend or is asking you to link into their network. Some people will befriend your friends to get to you or your company.
- Be wary of seemingly harmless quizzes. When someone invites you to take a survey, say, "10 Things Others Don't Know About You" or "My Favorite Things," it may be designed to harvest your data. The name of the street you grew up on or your favorite vacation spot could be clues to your passwords.
- Before you share any information anywhere online about yourself or your workplace, ask this question: What would the consequences be if this information fell into the hands of my boss, competitor or people who don't like me?



ChelseaGroton
Feel good about your bank.™

Member
FDIC

