2010 Survey of Consumer Protection in North Carolina

Consumer Scams, Identity Theft and Internet Safety

David Elliott, Director of Victims and Citizens Services
Consumer Protection Division
North Carolina Department of Justice

In 1969, the North Carolina General Assembly enacted G.S. § 75-1.1granting North Carolina's Attorney General powers similar to the Federal Trade Commission's powers to protect consumers from Unfair and Deceptive Trade Practices.

The Consumer Protection Division exercises the Attorney General's statutory authority in the areas of consumer protection, antitrust, utilities, and managed care. The Division works to protect consumers from fraud, deception, price fixing, price gouging, restraint of trade, commercial invasions of privacy, and other unfair and deceptive trade practices. It also represents the public in matters before the North Carolina Public Utilities Commission. The Division includes the Managed Care Patient Assistance Program, which advises patients who are experiencing difficulties with their managed care companies. Finally, the Division houses the Victims and Citizens Services Section (VCS) which aggressively develops and implements proactive strategies to address issues facing the citizens of North Carolina. These issues include:

- Consumer Protection
- ID Theft
- Internet Safety
- Child Abuse
- Open Government
- Juvenile Issues
- Sexual Assault
- Methamphetamine
- Domestic Violence
- Elder Abuse
- Victim's Rights
- Hate Crime Reporting

The primary responsibilities of the Division are: (1) the handling of consumer complaints; (2) investigating and prosecuting violations of the antitrust and consumer protection laws; (3) monitoring, commenting on, and occasionally drafting legislation that impacts North Carolina consumers, both at the state and federal levels; (4) assisting victims and educating North Carolinians about their rights as consumers; and (5) representing the consuming public before the Utilities Commission.

The Division consists of attorneys who specialize in various legal areas, consumer specialists and investigators, support staff, and three receptionists. Since 2001, the Division has handled an average of 17,000 written complaints per year. Approximately 100,000 telephone calls and a thousand email messages are processed each year.

Every year, the Division receives scores of calls from military personnel who have been victimized by unfair and deceptive practices. Like senior citizens, members of the military are disproportionately targeted. One consumer specialist is specifically charged with addressing issues related to the military community.

Complaint forms are available by calling (919) 716-6000 or (877) 566-7226 (toll free within N.C.). The forms can be submitted electronically or downloaded at http://www.ncdoj.com. Paper complaint forms should be mailed to:

North Carolina Department of Justice
Consumer Protection Division
9001 Mail Service Center
Raleigh, North Carolina 27699-9001

Attorney General Roy Cooper

Top 10 Consumer Tips

1. If it sounds too good to be true, it probably is.

2. Stop telemarketing calls. Add your phone number to the Do Not Call Registry at www.nocallsNC.com or call 1-888-382-1222 from the phone you wish to register.

3. Stop pre-approved credit offers from filling your mailbox by calling 1-888-5 OPT OUT (1-888-567-8688).

4. Review your credit report to see if you are a victim of identity theft. You are entitled to a free credit report each year from each national credit bureau. To get your free reports, go to www.annualcreditreport.com or call 1-877-322-8228.

5. Never share your Social Security number, credit card or bank account number or other personal information with someone who calls or emails you.

6. Walk away from high-pressure, act now or never sales tactics. Hang up on any telemarketer who won't take "NO" for an answer.

7. Read and understand all contracts before you sign them. Consult with a trusted family member, friend or lawyer if you have any questions.

8. Use a credit card when possible to pay for orders in advance. Using a credit card gives you some protection if your order doesn't arrive.

9. Don't pay money in advance for a loan or a prize. It's against the law for someone to charge an upfront fee on loans and prizes.

10. Check out a company with Attorney General Roy Cooper's Consumer Protection Division before you do business. You can also contact us for help if you've been the victim of a scam or bad deal. Call 1-877-5-NO-SCAM toll free within North Carolina.

Top 10 Consumer Myths

1. **MYTH:** You have a three-day right to cancel any purchase, including cars.

   FACT: The three-day right to cancel applies only to certain products, like gym memberships or dance lessons, or to certain kinds of sales, such as door-to-door sales or off-premise sales. Generally, your right to cancel is up to the company.

2. **MYTH:** Stores must give you a refund and must sell you an item for the advertised or posted price, even if it was a mistake.

   FACT: Some stores accept returns but they are not required to, so ask at the time of sale. Some will sell the item at the advertised price, but they aren't required to by law.

3. **MYTH:** Receiving an "Awards Notification" letter or call guarantees you've won a prize.

   FACT: Scammers use the promise of prizes to steal your money and personal information.

4. **MYTH:** The "Lemon Law" protects you on all big-ticket items, including used cars.

   FACT: North Carolina's lemon law only applies to new motor vehicles.

5. **MYTH:** Most of the money you give to a charity telemarketer is used for a charitable purpose.

   FACT: Some charities pay telemarketers as much as 90 cents of every dollar – so ask what percentage of your donation will benefit the worthy cause.

6. **MYTH:** Providing your credit card or Social Security number for identification or verification is OK if they say they are the government or your bank.

   FACT: Never share personal information when someone you don't know contacts you by phone or email. Instead, hang up and call the company or government agency at a number you know to be valid.

7. **MYTH:** You have a better chance of winning a publisher's sweepstakes if you buy magazines.

   FACT: Making a purchase isn't required and won't increase your odds of winning.

8. **MYTH:** People cannot take money out of your bank account without your written authorization.

   FACT: Keep your bank account and other personal information private to keep criminals from stealing your name and your money.

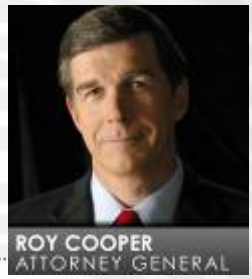
9. **MYTH:** Your credit report is private unless you authorize someone to see it.

   FACT: Creditors, such as banks and credit card companies, can check your credit report.

10. **MYTH:** Advertisements on the radio, TV, or in newspapers and magazines must be true.

    FACT: Ads are not always accurate. Read the fine print on ads and make sure a company has a good reputation before doing business with them.

ncdoj.gov



Identity Theft
Protect Yourself

GET FREE SECURITY FREEZES

A security freeze stops credit reporting agencies from releasing any information about you to new creditors without your approval, which can stop identity thieves from getting new credit in your name.

- All North Carolinians can get security freezes for free online. For more details, visit www.ncdoj.gov.
- Identity theft victims and seniors can also freeze their credit for free by mail or phone.
- Provide your full name, past home addresses, SSN, birth date, and two proofs of residence.
- To get a security freeze by mail or phone, contact the three major credit bureaus:

Equifax Security Freeze	**Experian Security Freeze**	**TransUnion Security Freeze**
PO Box 105788	PO Box 9554	PO Box 6790
Atlanta, GA 30348	Allen, TX 75013	Fullerton, CA 92834
1-800-685-1111	1-866-997-0418	1-888-909-8872

GET FREE YEARLY CREDIT REPORTS

- You are entitled to one free credit report from each of the three nationwide credit bureaus every year. To get your free reports, go to www.annualcreditreport.com or call 1-877-322-8228.
- To monitor your credit year round, ask for a free report from a different credit bureau every four months.

PROTECT YOUR SOCIAL SECURITY NUMBER

- Don't carry your Social Security card in your wallet.
- Give your Social Security Number (SSN) only when absolutely necessary.
- Ask why a SSN is needed, who will have access to it, and how it will be kept confidential.
- Don't print your SSN or driver's license number on your checks.

DESTROY DOCUMENTS YOU DON'T NEED

- Shred "pre-approved" credit card applications, old bank statements, insurance forms, etc.
- Learn about shred-a-thons in your area. Email alerts@ncdoj.gov and provide your county for updates or check the calendar at www.ncdoj.gov.

MONITOR FINANCES

- Limit the number of credit cards you carry.
- Copy credit cards (front and back) and keep them in a safe place in case a card is lost or stolen.
- Watch billing cycles for missing bills and review monthly statements carefully. Contact creditors if you miss a bill or if there are charges you don't recognize.
- Use automatic deposit for payroll, social security, or other federal benefit checks. Sign up for automatic deposit of federal checks by calling *Go Direct* at 1-800-333-1795.
- Review your Social Security Earnings and Benefits Statement for errors in your yearly salary. To order a statement, call 1-800-772-1213.

Protect Your Information Online

SURFING AND SHOPPING

- Keep spyware and virus protection software up-to-date, and install a firewall.
- Secure your wireless router and use the built-in encryption mechanism.
- Only provide your SSN or financial account numbers online through a valid, secure website. Secure websites often have an icon in the shape of a lock in the lower right-hand corner. A secure website's address will change from http to https.
- Pay for online purchases by credit card when possible. Federal law limits your liability to $50 maximum if your credit card number is lost or stolen. Paying by credit card can also give you a better chance of getting your money back if your order never arrives
- When ordering goods online, ask about refund policies, print order confirmations and keep track of delivery dates. It is best to order from trusted businesses or businesses that you confirm are legitimate.
- When selling items online, watch out for real-looking fake checks and money orders. Be wary of overpayments and endorsed checks. Never agree to wire excess payments back to the buyer or to someone else.
- Read privacy policies and inquire how your personal information will be used.
- Use one low-limit credit card for all online purchases or request a one-time-use number from your credit card company each time you want to make a purchase online.

EMAIL

- Beware of emails that ask you to confirm your personal information or account number, or that ask you to transfer money, even if the email appears to come from a bank, Internet Service Provider, business, or charity. Forward the email to spam@uce.gov.
- Never send your SSN or financial account numbers by email unless using encryption software.
- Be careful when clicking on links provided inside an email, even from a trusted source.
- Emails that say you've won the lottery, promise you can make a lot of money, or plead for help transferring money are almost always scams.

PASSWORDS

- Avoid PINs or passwords such as your mother's maiden name, family members' birth dates, your SSN or phone number, or a series of consecutive numbers (i.e., 1, 2, 3, 4).
- Combinations of letters, numbers, and special characters make the strongest passwords.
- Don't carry your PINs in your wallet or purse.
- Don't share PINs or passwords, even with close friends or relatives.
- Choose a different PIN for each account.

Watch Over Your Mail

- Stop pre-approved credit card offers by calling 1-888-5-OPT-OUT or visiting www.optoutprescreen.com.
- Place outgoing mail into a locked mailbox such as a blue postal service box.
- Don't leave incoming mail sitting in an unlocked mailbox.
- Cut down on unwanted mail by contacting the Direct Marketing Association at www.dmachoice.org.

Beware of Scams and Frauds

- Never give personal information to telemarketers who call you on the phone.
- Sign up for the national Do Not Call registry at 1-888-382-1222 or www.donotcall.gov to cut down on unwanted calls from telemarketers.
- Ask for and check references for door-to-door sales, home repair offers and other products.
- Verify that charities, businesses and others who contact you are who they claim to be before you provide any personal information. If you think the request for information is legitimate, hang up and contact the company at a number you know is valid to verify the request.
- Sign up for alerts about new scams at alerts@ncdoj.gov or by visiting www.ncdoj.gov.

INTERNET SAFETY

what you don't know can hurt your child

ROY COOPER
Attorney General

Online Risks

Computers and the Internet have revolutionized the way we communicate, work, shop and learn. But along with the positive changes come new dangers for young people including cyberbullying, online pornography, and adults who want to exploit them.

Secretive online communications between young people and adults can lead to seduction and sexual relations that are both harmful and illegal. For example, a 14-year-old North Carolina girl was enticed by a man she met on the Internet. Law officers examining the girl's computer found evidence of a 6-week online "romance." The man convinced the girl he loved her and couldn't wait any longer to be with her. She ran away from home and left the state on a bus with him.

Source: North Carolina State Bureau of Investigation

1 in 25 young people received an "aggressive" solicitation online in the last year from someone seeking a face-to-face meeting for sex

Survey of Internet users ages 10-17 *Source: National Center for Missing & Exploited Children*

The Latest Trend

Millions of young people have joined networking sites like MySpace and Facebook. These websites allow users to socialize with each other and when used safely they can be positive outlets for creativity and self-expression. But they can also expose young users to inappropriate material and adults who want to exploit them. Attorney General Roy Cooper tells parents and guardians the safest course is to keep children off of these sites.

However, parents who allow their child to use networking sites should read the site's safety tips, utilize its privacy settings, and provide extra supervision of their child's online activity. Remember, any part of the Internet that allows people to exchange messages can be used by adults trying to contact young people.

Teach Children to Avoid Risky Behavior

Young people who engage in risky online behaviors are more likely to receive sexual solicitations. These behaviors include visiting chat rooms, being rude or cruel to people online, and engaging in online activities with people they don't know. (Examples: Instant Messaging with strangers; sending personal information or photos to strangers; discussing sex online with strangers.)

Computer Tips

ESTABLISH FAMILY RULES

Create a set of family rules for computer use. To minimize resistance to these rules, try to put them into place before your children begin to go online. Include rules to govern which hours of the day your children can be online, how much time they can spend online each day, and others as you see fit. Ask your children to sign a pledge to follow these rules on every computer they use. (See pages 40 and 41 of the Attorney General's Resource Guide for Parents.)

CONTROL COMPUTER USE

Many experts believe that children should not have Internet access in their room, so place the computer your children use in a central location in your home. Explain that their use of the computer and the Internet is not private and that you will be monitoring their online activities. Parental Controls on your computer and those available through your Internet Service Provider can help supervise and monitor online activities. Additional monitoring software can also help.

DECIDE WHERE YOUR CHILDREN CAN GO ONLINE

Child-friendly search engines can help keep young members of your family safer online. Give each family member a separate login and password, then set up your parental controls to route your children's online search requests through a child-friendly search engine. (See the inside back cover of the Attorney General's Resource Guide for Parents.) As young people prove that they can use the Internet responsibly, parents can consider granting more freedom online.

Talk, Listen and Know

1. **TALK** to your children about computers and the Internet. In a calm manner, tell them about online dangers. Explain that they will have to follow your family's rules in order to be able to use the Internet. Rather than focusing on what they can't do, tell them about the things they will be able to do online if they use the Internet responsibly.
2. **LISTEN** to your children and keep lines of communication open. Encourage them to tell you if something happens online that makes them uncomfortable. Let them know you won't automatically pull the plug on their Internet activities. Most children don't tell their parents when they encounter dangers online because they fear they will lose Internet privileges.
3. **KNOW** what your children do online. Keep track of their online friends. Find out about the websites they visit. Monitor their activities to make sure they aren't straying from family rules they agreed to follow.

To learn more visit **www.ncdoj.gov**. Parents can view an Internet safety video and get a copy of the Attorney General's Resource Guide for Parents "Internet Safety: What You Don't Know Can Hurt Your Child."

To schedule an Internet safety presentation for parents, call 919-716-6783.

Monitoring Software

WHAT IS MONITORING SOFTWARE?

Monitoring software will help you to track your child's person's online activities on your home computer. This is done by purchasing a software program and installing it on the computer.

THINGS TO CONSIDER:

- Software is no substitute for supervision by a parent or guardian or for open communication with children and teens. Because parents cannot always be present when their child is online, monitoring software can be a valuable tool, but it cannot guard a child from potential risks that exist online.

- Monitoring software can provide information to help parents or guardians, such as what information a child makes available for others to see. It may tell you with whom they exchange instant messages (IM) online, what they chat about, which websites they visit, and how long they are online.

- Your computer may not be your child's only access point to the Internet. Internet access may be available in many locations — the library, school, or a friend's home — where there is not close adult supervision. It is important for parents to continually talk with their children about Internet safety and set clear expectations about online behavior.

- Talk with your child or teen about the installation of monitoring software. If you purchase monitoring software, NetSmartz411 recommends that you inform your child that the monitoring software is installed and talk with him or her about online safety. If your child does not know that the monitoring software is in place, he or she may feel as if his or her privacy has been invaded, and may be more resistant to discussing Internet safety concerns with you in the future. Emphasize that you trust your child or teen to make responsible decisions online. Explain your reasons for using the software and encourage your children to come to you if they encounter something online that makes them scared or uncomfortable.

HOW DO I SELECT THE RIGHT MONITORING SOFTWARE FOR MY FAMILY?

Choosing the right monitoring software for your family can be difficult. There are many available and each one works a little differently. Here are some things to consider when selecting one.

- Ease of use:
    - Is it easy to install?
    - Can it be easily monitored?
    - Is it easy to tell if it is not working?
- Effectiveness: Is it effectively monitoring your child's activities?
- Recording: Does it record keystrokes, web surfing, chat, and file transfers?
- E-mail logging: Does it log your child's e-mails? Does it log e-mail attachments?
- IM logging: Does it log all programs your child uses?
- Visuals: How does it show you your child's activities?
- Customization: Can you customize it to fit the needs of your family?
- Management: Can you monitor it from other computers?

Product reviews:

Find out how others have rated the product before purchasing it. While we do not endorse any particular product, you may find reviews of different monitoring software at **www.getnetwise.org** and **http://www.consumerreports.org/www.consumerreports.org**.

To view a list of top ten monitoring software products, go to **http://monitoring-software-review.toptenreviews.com**.

You may also want to look in a local electronics or computer store, use search engines online to look for the software, or check with your Internet service provider for suggestions.

Monitoring software information from Netsmartz411, the Internet safety helpdesk of the National Center for Missing & Exploited Children.
Provided courtesy of Attorney General Roy Cooper.

Safer Social Networking

Children use social networking sites to create their online identity, communicate with their friends, and meet people with similar interests. Like most new technological developments, this brings both positive and negative implications. Social networking sites incorporate instant messaging, chatrooms, profiles, pictures, E-mail, and blogging all in one site. Here are some tips to help keep children safer while they are using social networking websites like Facebook, MySpace, or Xanga.

TIPS FOR PARENTS AND GUARDIANS

Talk to your children about:

- the possible risks and future repercussions
- their online activities. View their profile or blog together. If your child is not willing to do this, then your child may have information on their blog or profile they do not want you to see and should not have posted
- not giving out personal information, such as names, school, city, or e-mail address. This includes making or posting plans and activities on the site
- posting pictures online. Once an image is posted anywhere on the Internet (even on a profile with private settings), it may never be completely erased from the Internet, even if it is deleted
- the dangers of communicating with people they have never met in person. Remind them that people on the Internet are not always who they say they are
- coming to you or another trusted adult if he or she ever feels threatened or uncomfortable about something online
- using privacy settings to restrict who can and cannot access their profile or blog. Teach children to only accept people as friends if they know and trust them in real life

Monitor what your child's friends are posting regarding your child's identity. Often children and their friends have accounts linked to one another, so it's not just your child's profile and information you need to worry about.

Familiarize yourself with the social networking website’s features and safety tips.

Report any illegal content to:

1. Appropriate law-enforcement agencies
2. CyberTipline.com
3. Your Internet service provider
4. The social networking website’s webmaster

TIPS FOR KIDS AND TEENS

Never post your personal information, such as cell phone number, address, or the name of your school.

Be aware that information you give out in blogs could also put you at risk of victimization. People looking to harm you could use the information you post to gain your trust. They can also deceive you by pretending they know you.

Never give out your password to anyone other than your parent or guardian. Only add people as friends to your site if you know and trust them in real life.

Never meet in person with anyone you first "met" on a social networking site. Some people may not be who they say they are.

Think before posting your photos. Personal photos should not have revealing information, such as school names or locations. Look at the backgrounds of the pictures to make sure you are not giving out any identifying information without realizing it. The name of a mall, the license plate of your car, signs, or the name of your sports team on your jersey or clothing all contain information that can give your location away.

Never respond to harassing or rude comments posted on your profile. Delete any unwanted messages or friends who continuously leave inappropriate comments. Report these comments to the networking site if they violate that site's terms of service.

Use the privacy settings of the social networking site:

- Set it so that people can only be added as your friend if you approve it
- Set it so that people can only view your profile if you have approved them as a friend

Remember that posting information about your friends could put them at risk. Protect your friends by not posting any names, ages, phone numbers, school names, or locations. Refrain from making or posting plans and activities on your site.

Consider going through your blog and profile and removing information that could put you at risk. Remember, anyone has access to your blog and profile, not just people you know.

More information about safer blogging is available in the NCMEC publication ***Blog Beware***. Although the purpose of a social networking website is to meet people with similar interests and to swap information, it is important to ensure your child understands that these sites carry some risks along with the benefits. Communicating with your child is an important and effective strategy for keeping them safer. Talk with your children frequently, ask questions about their online activities, and regularly take a look at their profiles or blogs.

Social networking information from Netsmartz411, Internet safety helpdesk of the National Center for Missing & Exploited Children.
Provided courtesy of Attorney General Roy Cooper.

Social Networking

BLOCKING ACCESS

Filtering software can be used to block your child's access to MySpace and certain other websites; a filter is a software product that controls the websites or places online your child is allowed to visit. It can also restrict children from downloading files from the Internet, as well as control the amount of time a child or teen is online.

Although filtering software can be beneficial and helpful, filters are not foolproof. While it can prevent children from accessing certain subjects, keep in mind that filters are not a substitute for parental supervision. Most filters are fairly good at blocking websites containing content that parents and guardians do not approve of, but some websites containing questionable content can get past filters. Also, sometimes filters can be restrictive and block access to sites that do not contain questionable content.

DELETING MY CHILD'S MYSPACE PROFILE

If you are a parent or guardian and you want help with your child's profile, e-mail parentcare@myspace.com.

To remove your child's account using his/her log-in information

- Log into your child's MySpace account
- Click on "Account Settings"
- Click on "Cancel Account" near the top
- Click on the red button that says "Cancel Account"
- Enter the reason as "parent deleting"
- Click "Cancel Account" again
- An e-mail will be sent to the user's e-mail account verifying deletion
- Click on the link to confirm the cancellation

If you do not receive this e-mail, remove all content from your child's profile by clicking on "Edit Profile" then deleting all information. Type "remove profile" in the "About Me" section, then contact MySpace with the URL of your child's page and it will be removed.

If your child will not work with you to remove the account

Send an e-mail to customercare@myspace.com, making sure to include your child's MySpace URL and a message to explain your situation.

To report a profile as an underaged user

Users must be 14 to join MySpace. If you see underaged users on MySpace, contact MySpace with the profile's URL or friend ID number. It will be removed if MySpace finds that this user is misrepresenting his or her age. To report underaged users, e-mail underagereport@myspace.com.

Social networking information from Netsmartz411, Internet safety helpdesk of the National Center for Missing & Exploited Children.
Provided courtesy of Attorney General Roy Cooper.

SAMPLE QUESTIONS ANSWERED AT NETSMARTZ411

What is a social networking site?

Are websites like MySpace and Facebook safe for my kids?

MYSPACE

How do I contact MySpace?

How do I access my child's MySpace profile?

Is MySpace safe for teens if they set their profiles so only invited friends can see them?

How do I set a profile on MySpace to private?

Someone is posting my child's picture on MySpace without my permission. What can I do?

My daughter's MySpace page hides her friends and comments. How can I access this information?

My 14 year old received MySpace e-mails from a 29 year old asking if she wanted to see explicit pictures of him. What do I do?

FACEBOOK

Is Facebook only for users in college?

How do I report abuse on Facebook?

Can users post comments anonymously on Facebook?

How do I access my child's Facebook profile?

How do I use privacy settings on Facebook?

OTHER

Are faith-based social networking sites safe?

Is it unsafe to post family pictures of children online?

What do teens do online? Do they think about safety?

What is Club Penguin? Is it safe for kids?

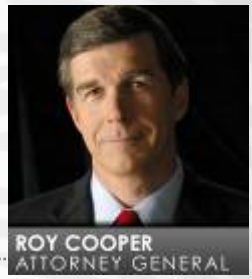
What is weeworld.com? What are the risks?

How do I limit access to the Internet on a PSP?

What do online abbreviations/acronyms mean?

Should my child or teen have a cell phone? What are the risks?

ncdoj.gov



Received a Security Breach Letter?

Under North Carolina law, businesses and state and local government agencies must notify you if your personal information was compromised and if you are at greater risk of identity theft.

What Is a Security Breach?

A security breach happens when data or records containing personal information such as Social Security numbers, bank account numbers or drivers license numbers are lost, stolen, or accessed improperly. This kind of information can be used by criminals to commit identity theft.

Being notified that your information was part of a security breach does not necessarily mean you will become a victim of identity theft. However, you are at a greater risk and need to take steps to protect yourself.

Step 1: Sign Up for Free Services

Some businesses or government agencies offer security breach victims a free service such as credit monitoring. While most offers are genuine and should be utilized by the victim, do not provide private information to the number provided without independently verifying that the credit monitoring service or other business is legitimate.

Step 2: Notify the Credit Bureaus

A fraud alert tells banks and other creditors to take extra steps to verify your identity before issuing credit in your name, but it will not stop new credit in your name. A fraud alert is free and will last 90 days unless you request an extended seven-year fraud alert and provide a police report.

To request a fraud alert, contact one of the three nationwide credit bureaus. The alert will be shared and a flag will be placed on your credit file with all three. Each credit bureau provides you with a free credit report. Review these reports carefully for any fraudulent activity and notify the credit bureaus online or in writing of any discrepancies.

- www.Equifax.com – 1-800-525-6285
- www.Experian.com – 1-888-397-3742
- www.TransUnion.com – 1-800-680-7289

Step 3: Consider a Security Freeze

A security freeze stops access to new credit in your name. Placing a security freeze prohibits credit reporting agencies from releasing any information about you to new creditors without your approval, making it difficult for an identity thief to use your information to open an account or obtain credit. A security freeze is free for victims of identity theft who provide a copy of a police report.

To place a freeze, send a letter by certified mail to each of the credit bureaus that includes the following information along with payment:

- Full name including middle initial and any suffix (such as Jr.)
- Home addresses for the last five years
- Social Security Number and date of birth
- Two proofs of residence (examples: copy of driver's license, utility bill, insurance statement, bank statement)
- Police or DMV report if you're a victim of identity theft
- If there is no police report, send $10 payment by check, money order, or credit card (TransUnion accepts payment by credit card only) All credit bureaus accept Visa, Master Card, American Express, or Discover. Please include card name, account number and expiration date, and the card identification number on the back of the card.
- A sample letter is available at www.noscamnc.gov.

Equifax Security Freeze	**Experian Security Freeze**	**TransUnion Security Freeze**
PO Box 105788	PO Box 9554	PO Box 6790
Atlanta, GA 30348	Allen, TX 75013	Fullerton, CA 92834

*Innovis is not a nationwide credit bureau but does permit security freezes by following the same instructions and mailing the information to P.O. Box 725, Columbus, Ohio 43216.

For detailed instructions about the security freeze, see our tip sheet, "Freeze Access to Your Credit," at www.noscamnc.gov.

Step 4: Monitor Your Credit Report

Continue to review your credit reports every few months. Your private information may not be used immediately so watch over your file regularly. You can request a free credit report annually by calling 1-877-322-8228 or going online at www.annualcreditreport.com.

Notifying Law Enforcement

Most law enforcement will not issue you a police report until your private information is actually used. If you have any suspicion that your private information is being used, contact local law enforcement immediately. Filing a police report triggers helpful protections under both federal and state law, such as an extended fraud alert and a free security freeze. A police report will be useful as you contact creditors to try to restore your credit. Request a copy of the police report and keep a copy in your files.