GENESEO POLICE DEPARTMENT

119 MAIN STREET, GENESEO, NEW YORK 14454
TEL 585-243-2420 / FAX 585-243-2443

Identity Theft Prevention

There are many ways you can go about protecting yourself from identity theft. Practicing these prevention techniques will help to increase the safety of your identity.

1. **Monitor your finances**
   Frequently check your bank and credit accounts for suspicious activity, such as unusual withdrawals and payments. Pay attention to your credit report as fraudulent activity may affect your score. You can get a free copy of your credit report once a year at ***annualcreditreport.com*** or call 1-877-322-8228. The three credit reporting agencies can be found at ***equifax.com, experian.com*** and ***transunion.com***. *Sign up for text alerts with your credit card company so each time your card is used you are notified.*

2. **Never leave personal information unsecured.**
   A locked car is not a secure location. Identity thieves target trail heads, gyms, day care centers, and other locations where it is likely people will not bring their purses or wallets with them. A purse or wallet without any cash could still be worth over $10,000 in personal documents and credit cards. If you donôt feel comfortable leaving $10,000 somewhere do not leave your identity there.

3. **Watch for Scams**
   Scammers are constantly coming up with new ways for stealing your identity and getting your cash. If someone is offering you something for nothing or a deal sounds too good to be true it may be a scam. If you have to deposit a check and/or wire money it may be a scam. Also be aware of romance scams, lottery scams, IRS scams, hostage scams, and scams inducing people to part with their money through social engineering schemes.

4. **Practice safe Email, Text and phone etiquette**
   Do not respond to requests for personal information through email, text or over the phone. Companies and government agencies that have a legitimate interest will not contact you this way. Never go to a link or open an attachment if you do not need to.

5. **Shred sensitive documents before discarding**
   Thieves can easily search through your garbage to find documents with personal information. Before throwing out old bills, bank statements, receipts or other items that may contain this information make sure to shred them so that they cannot be read.

6. **File your taxes as early as possible.** Last year $6 billion in fraudulent tax returns were filed. Reduce the chances you or one of your dependents will be targeted by filing as early as possible.

7. **Be cautious when using ATMs**
   Check to make sure that an ATMôs card slot is legitimate and not temporarily or unofficially attached to the machine. Some scammers utilize ñskimmers,ò devices designed to steal card information through its magnetic strip. Scammers will also place hidden cameras overlooking key pads in order to steal your PIN number. To avoid this try to use familiar ATMs, limit the amount of transactions you make and *shield the keypad with your hand when punching in numbers.*

8. **Use care at the pump**
   Skimmer devices can be attached to both the inside and outside of a gas pump and connected to the magnetic strip reader.
   - The easiest way to avoid gas pump skimmer devices is to pay inside the gas station instead of at the pump.
   - When paying consider using a credit card instead of a debit card. Credit cards usually have better fraud protection and the money is not immediately deducted from your bank account.
   - If available use the closest gas pump to the attendant as they are the least likely to have been tampered with. Also, try not to use pumps that are out of the attendantôs sight or poorly lit.
   - Some gas stations use security stickers on pump access doors. Avoid pumps that have damaged security seals and report issue to attendant.
   - Consider using a prepaid card that you keep a limited dollar amount on.
   - When in doubt use cash when purchasing gas.
   - If you see any suspicious activity or people around the pumps please call 911 or notify the gas station attendant.

9. **Watch your mail**
   Donôt leave mail in your mailbox for extended periods of time. Bills and incoming checks contain sensitive personal information that can easily be stolen if left unattended. If you know you are going to be away from home for a long amount of time you can call your local post office and set up a vacation hold so that no mail will be delivered until you return (You can set up a hold electronically by visiting ***holdmail.usps.com****). You should also take all outgoing checks and mail containing personal information to the post office or nearest post office collection box and never leave them in your mailbox.*

10. **Opt-Out of Unsolicited Credit and Insurance Offers**
    Although identity theft through pre-approved credit and insurance offers is rare it is still possible. You can reduce the number of unsolicited credit and insurance offers you receive by placing yourself on the federal governments National Do Not Call Registry. To register your phone number or to get more information you can call ***1-888-382-1222*** or visit ***donotcall.gov***. You can also visit the official Consumer Credit Reporting Industry website ***optoutprescreen.com*** or call ***1-888-5-OPT-OUT***.

11. Protect Your Electronic Devices

Your computer, laptop, cell phone, tablet, gaming device and online accounts can contain everything a thief needs to steal your identity.

- Make sure to create passwords that mix letters, numbers and special characters. Change them often and do not use the same password for more than one account.
- Keep up to date antivirus software installed on your devices at all times.
- Never click on any links or attachments you are not sure of.
- Confirm that your computer is only communicating over a secure connection. Do not connect to secure accounts, such as your bank or email, when you are connected to an unknown or public Wi-Fi network.
- Thieves can create fake websites that mirror legitimate ones in order to steal personal information. Whenever you are shopping online or entering sensitive information check to see if the web address begins with ñhttps.ò This means that the website you are on is secure.

12. Safe Social Networking

Social networking through sites such as Facebook, Twitter and LinkedIn has become a major part of many peopleôs lives. These sites are a great way to stay connected with friends and family but you should be cautious about how you use them.

- Anything you post online is permanent even if you delete it. Information such as your address, phone number and birthday are all things scammers can use to steal your identity. One common way that hackers break into accounts is through the ñForgot Passwordò link on the login page. Sharing the answers to your security questions, such as the names of your pets and where you went to high school, can give hackers easy access to your accounts.
- Be selective when accepting friends. Make sure you really know them and it is them requesting.
- Manage your privacy settings. Only share information with friends and family. Regularly check your privacy settings to make sure that they havenôt changed. Sometimes social media accounts will automatically link with one another, sharing your information. If you post information that you do not want shared between accounts make sure to disable this feature before sharing anything.

For more information on identity theft and to find out what to do if someone has stolen your identity visit:

- Federal Trade Commission
  - *FTC.gov/IDTheft*

- Federal Bureau of Investigation
  - www.fbi.gov

- U.S. Department of Justice
  - www.usdoj.gov/whatwedo/whatwedo_if.html

- Office of the Attorney General
  - www.oag.state.ny.us/resource_center/resource_center.html

- Credit Report Agencies
- Equifax: www.equifax.com

- Experian: www.experian.com
  - *experian.com/fraud/center*

- TransUnion: www.transunion.com
  - *transunion.com/personal-credit/credit-disputes/fraud-alerts.page?*

- *justice.gov/criminal-fraud/report-fraud* or call *1-877-ID-THEFT*

- The Internet Crime Complaint Center (IC3)
  - www.ic3.gov
- Office of the Inspector General, Social Security Administration
  www.oig.ssa.gov Hotline #: 1-800-269-0271

IDENTITY THEFT VICTIM QUICK RESPONSE CHECKLIST

- ✓ **REPORT FRAUD IMMEDIATELY TO THE THREE MAJOR CREDIT REPORTING BUREAUS BY CALLING THE TOLL-FREE NUMBERS BELOW:**
  - **Experian 1-888-397-3742**
  - **Equifax 1-800-525-6285**
  - **TransUnion 1-800-680-7289**

- ✓ **REQUEST YOUR FREE CREDIT REPORTS AND REVIEW THEM FOR ANY INACCURACIES**
  - **Consumers are entitled to one free credit report annually from each of the three major credit bureaus. Victims of ID Theft are entitled to another free copy. Look for accounts you don't recognize. Check the inquiries section for names of creditors from whom you haven't requested credit.**

- ✓ **REQUEST A FREE COPY OF YOUR POLICE REPORT**
  - **Go to your local police station and give the police as much information on the theft as possible. Under the law, you are entitled to a free copy of the report.**

- ✓ **CALL YOUR BANK, OTHER CREDITORS, UTILITY COMPANIES, AND THE DEPARTMENT OF MOTOR VEHICLES WHERE NECESSARY, TO ALERT THEM TO THE IDENTITY THEFT AND FOLLOW-UP IN WRITING WITH A COPY OF THE POLICE REPORT**
  - **Ask for the security or fraud department to report the theft and to open new accounts with new account numbers. Tell creditors that you want a new password to access each of your new accounts.**

- ✓ **CONSIDER PLACING A CREDIT FREEZE ON YOUR CREDIT REPORT**
  - **The strongest protection against new accounts being opened in your name is a credit freeze also called a security freeze which ensures that credit reports cannot be accessed without your permission.**

New York State
CONSUMER PROTECTION BOARD
Advocating for And Empowering NY Consumers
1-800-697-1220
WWW.NYSCONSUMER.GOV

New York State
DIVISION OF CRIMINAL JUSTICE SERVICES
ENHANCING PUBLIC SAFETY AND IMPROVING CRIMINAL JUSTICE
1-800-262-3257

THE FBI FEDERAL BUREAU OF INVESTIGATION

Common Fraud Schemes

Internet Fraud

Listed below are tips to protect yourself and your family from various forms of Internet fraud.

For information on the most common complaints and scams, see the annual reports of the Internet Crime Complaint Center, or IC3, a partnership of the FBI and the National White Collar Crime Center. Also see its information on Internet Crime Schemes and its Internet Crime Prevention Tips.

Use our online tips form or the IC3 website to report potential cases of cyber fraud.

Tips for Avoiding Internet Auction Fraud:

- Understand as much as possible about how the auction works, what your obligations are as a buyer, and what the seller's obligations are before you bid.
- Find out what actions the website/company takes if a problem occurs and consider insuring the transaction and shipment.
- Learn as much as possible about the seller, especially if the only information you have is an e-mail address. If it is a business, check the Better Business Bureau where the seller/business is located.
- Examine the feedback on the seller.
- Determine what method of payment the seller is asking from the buyer and where he/she is asking to send payment.
- If possible, purchase items online using your credit card, because you can often dispute the charges if something goes wrong.
- Be cautious when dealing with sellers outside the United States. If a problem occurs with the auction transaction, it could be much more difficult to rectify.
- Ask the seller about when delivery can be expected and whether the merchandise is covered by a warranty or can be exchanged if there is a problem.
- Make sure there are no unexpected costs, including whether shipping and handling is included in the auction price.
- There should be no reason to give out your social security number or driverôs license number to the seller.

Tips for Avoiding Non-Delivery of Merchandise:

- Make sure you are purchasing merchandise from a reputable source.
- Do your homework on the individual or company to ensure that they are legitimate.
- Obtain a physical address rather than simply a post office box and a telephone number, and call the seller to see if the telephone number is correct and working.
- Send an e-mail to the seller to make sure the e-mail address is active, and be wary of those that utilize free e-mail services where a credit card wasn't required to open the account.
- Consider not purchasing from sellers who won't provide you with this type of information.
- Check with the Better Business Bureau from the sellerôs area.
- Check out other websites regarding this person/company.
- Donôt judge a person or company by their website. Flashy websites can be set up quickly.
- Be cautious when responding to special investment offers, especially through unsolicited e-mail.
- Be cautious when dealing with individuals/companies from outside your own country.
- Inquire about returns and warranties.
- If possible, purchase items online using your credit card, because you can often dispute the charges if something goes wrong.
- Make sure the transaction is secure when you electronically send your credit card numbers.
- Consider using an escrow or alternate payment service.

Tips for Avoiding Credit Card Fraud:

- Don't give out your credit card number online unless the site is a secure and reputable. Sometimes a tiny icon of a padlock appears to symbolize a higher level of security to transmit data. This icon is not a guarantee of a secure site, but provides some assurance.
- Don't trust a site just because it claims to be secure.
- Before using the site, check out the security/encryption software it uses.
- Make sure you are purchasing merchandise from a reputable source.
- Do your homework on the individual or company to ensure that they are legitimate.
- Obtain a physical address rather than simply a post office box and a telephone number, and call the seller to see if the telephone number is correct and working.
- Send an e-mail to the seller to make sure the e-mail address is active, and be wary of those that utilize free e-mail services where a credit card wasn't required to open the account.
- Consider not purchasing from sellers who won't provide you with this type of information.
- Check with the Better Business Bureau from the sellerôs area.

- Check out other websites regarding this person/company.
- Donôt judge a person or company by their website. Flashy websites can be set up quickly.
- Be cautious when responding to special investment offers, especially through unsolicited e-mail.
- Be cautious when dealing with individuals/companies from outside your own country.
- If possible, purchase items online using your credit card, because you can often dispute the charges if something goes wrong.
- Make sure the transaction is secure when you electronically send your credit card number.
- Keep a list of all your credit cards and account information along with the card issuerôs contact information. If anything looks suspicious or you lose your credit card(s), contact the card issuer immediately.

Tips for Avoiding Investment Fraud:

- Donôt judge a person or company by their website. Flashy websites can be set up quickly.
- Donôt invest in anything you are not absolutely sure about. Do your homework on the investment and the company to ensure that they are legitimate.
- Check out other websites regarding this person/company.
- Be cautious when responding to special investment offers, especially through unsolicited e-mail.
- Be cautious when dealing with individuals/companies from outside your own country.
- Inquire about all the terms and conditions.

Tips for Avoiding Business Fraud:

- Purchase merchandise from reputable dealers or establishments.
- Obtain a physical address rather than simply a post office box and a telephone number, and call the seller to see if the telephone number is correct and working.
- Send an e-mail to the seller to make sure the e-mail address is active, and be wary of those that utilize free e-mail services where a credit card wasn't required to open the account.
- Consider not purchasing from sellers who won't provide you with this type of information.
- Purchase merchandise directly from the individual/company that holds the trademark, copyright, or patent.

Tips for Avoiding the Nigerian Letter or “419” Fraud:

- Be skeptical of individuals representing themselves as Nigerian or foreign government officials asking for your help in placing large sums of money in overseas bank accounts.
- Do not believe the promise of large sums of money for your cooperation.
- Guard your account information carefully.

Welcome to IC3

The Internet Crime Complaint Center (IC3) is a partnership between the Federal Bureau of Investigation (FBI), the National White Collar Crime Center (NW3C), and the Bureau of Justice Assistance (BJA).

IC3's mission is to serve as a vehicle to receive, develop, and refer criminal complaints regarding the rapidly expanding arena of cyber crime. The IC3 gives the victims of cyber crime a convenient and easy-to-use reporting mechanism that alerts authorities of suspected criminal or civil violations. For law enforcement and regulatory agencies at the federal, state, local and international level, IC3 provides a central referral mechanism for complaints involving Internet related crimes.

Filing a Complaint with IC3

IC3 accepts online Internet crime complaints from either the person who believes they were defrauded or from a third party to the complainant. We can best process your complaint if we receive accurate and complete information from you. Therefore, we request that you provide the following information when filing a complaint:

- Your name
- Your mailing address
- Your telephone number
- The name, address, telephone number, and Web address, if available, of the Individual or organization you believe defrauded you.
- Specific details on how, why, and when you believe you were defrauded.
- Any other relevant information you believe is necessary to support your complaint.

File a Complaint >> http://www.ic3.gov/default.aspx