TABLE of CONTENTS

Suffolk County Police Department
Identity Theft Unit
30 Yaphank Avenue
Yaphank, NY 11980
Phone: 631-852-6821
E-mail: Identity. Theft @ suffolkcountyny.gov
http://www.co.suffolk.ny.us/police/specialunits.htm

As a part of its community outreach program, The Identity Theft Unit provides speakers for presentations to the public about the dangers of identity crimes and tips on how to avoid becoming a victim. If your organization is interested in hosting such an event please contact the unit at 631-852-6821.

Commanding Officer Detective Sergeant Stephen C. Jensen

Prepared by: Dorothy Morelli, Research Analyst

WHAT IS IDENTITY THEFT?

Identity theft occurs when someone uses your:

- Name
- Date of Birth
- Social Security Number
- Maiden Name
- Other personal identifying information

to commit a crime or a fraud.

Most folks only consider identity crime as being financial, but an imposter can just as easily identify himself as you when he is arrested for non-financial crimes, such as driving while under the influence. Some criminals may also use your personal identifying information to obtain passports or driver's licenses in your name, a scenario that may have national security aspects if the criminal(s) are connected to terrorism.

WHAT CRIMINALS DO WITH YOUR IDENTITY

- Open New Accounts
  - bank accounts
  - credit/debit card accounts
  - cell phone and utility
- Take over your existing accounts.
- Clone your credit and debit cards
- Obtain loans
  - home mortgages
  - equity lines
  - auto financing
- Counterfeit your checks.
- Commit crimes in your name

THE FIRST LINE OF DEFENSE IS YOU!

An important aspect to remember about the theft of identities, while large scale data breaches of merchant and financial institution computer databases is a reality, the identity thief in most cases employs more traditional, low-tech methods to steal your information. This knowledge places the ability to prevent identity theft in the hands of the potential victim, who can make informed decisions about the security of his or her personal information. So it is very important that you know how identity thieves can obtain your personal identifying information.

HOW ARE IDENTITIES COMPROMISED?

- **VICTIM ASSISTED:** The victim divulges personal information to anyone who asks for it whether or not the information is required even during cash transactions, or through scams designed to encourage the victim to give out personal data.
  - Pretext phone calls
    - These are phone calls made by criminals meant to trick the intended victim into divulging personal information.
    - Often the caller leads the victim to believe he represents a lottery or a financial institution and needs your personal information so you can claim a prize or to update personal account data at your bank.
  - Store clerks / office receptionists
    - Often request personal information from a customer or a patient when not required to deliver the service or merchandise.
- **THEFT OR LOSS OF:**
  - Wallets and pocketbooks
  - Mail
  - Trash containing personal information
  - How much personal identifying information is in your wallet or thrown out in the trash?

- **BURGLARY:** of residence or business where personal information may be stored
  - **Is your personal information kept in a safe, secure place?**

- **SKIMMING**
  - An identity thief can obtain a victim's credit card number as easily as just copying down the victim's credit card number. A more advanced method used by criminals is to employ a small electronic device, called a skimmer, to swipe and store hundreds of victims' credit card numbers. Common scenarios for skimming are restaurants or bars where the skimmer has possession of the victim's credit card out of their immediate view.
    Skimming may also involve placing a device over the card slot of an ATM (Automated Teller Machine), which reads the magnetic strip as the user unknowingly passes their card through it. A pinhole camera or fake keypad may be utilized to record the user's PIN at the same time.
- **INTERNET**
  - "Phishing"
    - "Phishing" is an e-mail message that appears to be sent by a legitimate institution designed to trick consumers into divulging personal information – such as their credit or debit account numbers, checking account information, Social Security numbers or banking account passwords – by directing the recipient to a fake website or prompting a reply e-mail.
  - Unsecured wireless networks
    - As more people install wireless routers on their home computer networks they fail to utilize the security features on their wireless routers or firewall software.
      Criminals can gain access to a victims unsecured internet connection and use it to commit crime and frauds.
  - Unsecured laptops using "hotspots"
    - Criminals can gain access to your laptop while you use a public "hotspot" and obtain personal or important information stored in files on the laptop's hard drive
  - Fake websites
    - Fake websites mimic the sites of established companies to trick prospective customers into revealing credit card information.
    - Look for the security indicators on your web browser such as, the Padlock symbol and "http**s**" in the address box.

PREVENTION TIPS

- ***Vigilance = Protection!***
- **You Decide When and What Information You Want To Give Out**
  Ask a merchant or service provider requesting your Social Security number or personal information:
  - Why do they need it?
  - What will they do with it?
  - Where will it be kept?
  - Will you still get the merchandise or service if you do not provide them with your personal information?
  - Can you substitute passwords or identifiers of your choosing?
- **DO NOT** give out personal information over the phone or Internet unless you initiate the communication to a known person or business.
- **DO NOT TRUST** caller id's to identify the caller. The advent of Voice over Internet Protocol (VOIP) Phone Service allows the criminal to "spoof" or fake the displayed number.
  - **Financial institutions will not phone or e-mail you requesting personal information regarding your accounts or other personal identifying information.**

- **Wallet or Pocketbook**
  - Only carry the personal information you need daily in your wallet or purse.
  - Leave your **Social Security Card** in a safe place at home.
  - Reduce the number of credit cards you carry – better yet, only take a credit card with you when you expect to use it. Secure extra credit cards in a safe place at home.
  - **DO NOT** keep copies of Social Security numbers, account numbers, PINS or other identifying information in your wallet or address book.
  - You must carry your driver's license and in many cases business or school identification as well as health insurance cards. Such documents may contain your **Social Security number**. If possible, replace your Social Security number with a different identifying number or password.
- **Protect your mail**
  - Locking mail boxes.
  - Vacation holds on mail delivery.
  - Outgoing mail should only be placed in U.S. Postal Service collection boxes.
  - Opt Out of receiving pre-screened credit offers. (See the resource page for information on Mail Solicitations.)
  - Know your billing cycles so you know when your bill is late or stolen.
- **Trash:** Shred documents containing personal information before placing in the trash. **IF IN DOUBT, SHRED IT!**
- **DO NOT CARRY Passwords** for credit, debit cards, bank and phone accounts in your wallet, pocketbook or day planner. Do not write the PIN on your credit/debit cards.
- **Secure Your Information**
  - At home – burglar proof by storing personal information and valued items in secure areas.
  - Know who has access to your information such as **family, friends and home assistants.** Take action to secure your information from those who you do not want to have access.
- **Order your Credit Bureau Reports**
  - Check your credit reports carefully for credit cards and loans you may not have opened or applied for. (See the enclosed Resource Page for information on the three (3) major Credit Reporting Agencies.)

YOUR COMPUTER AND IDENTITY THEFT

Computers with access to the internet can be found in almost every household and business in Suffolk County. The technology offers growing opportunities to communicate, educate, and conduct business from homes and businesses in a way that was beyond our imaginations just a short time ago. The speed of technological advances in the area of home and office computing often surpasses the user's ability to comprehend and fully use all the computer's features especially when it comes to security.

As users become more involved in on-line banking, commercial purchases and other e-businesses, the risks for the loss or theft of personal information has become a matter of concern. There are many stories by the news media about the theft of customer or client information through huge corporate data breaches but, you should not forget that your personal computer may also be the target of attack by identity thieves. The following tips are offered to get you thinking about secure computing and on-line habits.

Social Networking Sites

Social Networking sites such as My Space, Facebook, You Tube and Twitter, as well as others, are on-line communities that offer new and exciting venues for users to meet new people or maintain communication with on-line friends or groups. Your information can be entered as a user profile, or dialogue in bulletins or **blogs**. As in any real world community, the criminal element has found a way to lurk in the shadows to exploit the unwitting or careless for their own benefit or to cause harm.

Users should be mindful that the personal information they list on their on-line profile in these communities may be open for everyone in the community to see. Though you may feel that the information by itself cannot be used to harm you, it should be considered in the context of all the information you slowly provide over time through blogging and bulletins.

- Consider limiting the information listed on the site's profile page. The compromise of personal information is a very real issue when using social networking sites.
- Learn to use the networking site's security features such as Facebook's "Friends List" that limits who can access your page.
- Carefully consider what photo's you wish to post, not only for memorializing potentially embarrassing incidents but what information a criminal can learn about you from the background, such as school banners, or the room's furnishings.
- Networking sites may be a source for computer viruses, Trojan Horses and Spyware
- Networking sites have been used to spread "phishing" e-mails or change site content without your authorization.
- Do not take for granted that the networking site's security features work.

Online Safety:

- **Computer Security**
  - Use antivirus software.
  - Use or enable firewall software.
  - Keep your Operating System and virus software updated.
  - Beware of e-mail attachments from those you don't know.
  - Turn the computer off when not in use.
  - Use a strong password containing both upper and lower case letters and numbers.
  - If using a router, keep security firmware updated.

- **Wireless Networks**
  - Wireless networks, either in the home or in a business, present computer safety issues most users do not encounter while using their "wired" internet connections. One of these dangers may include what is commonly called "war driving", where criminals and hackers may gain access to your internet connection because it is broadcasted outside your home. Thieves may not only gain access to the internet but to your computers' hard drive where you may have stored important personal identifying information. Criminals can use your internet connection to commit crimes on the internet which can be traced back to your home address.
    - Make sure you change the default password after installation.
    - Change the default SSID (Service Set Identifier; it is referred to as a network name because it essentially is a name that identifies a wireless network) – **change** it frequently.
    - Disable SSID Broadcast.
    - Enable Wireless Security (WEP or WAP).
    - Keep the wireless router firmware updated.

- **Laptop Computers**
  - If possible **DO NOT** store personal data on a laptop.
  - Consider Physical Security.
    - Locks
    - Security cables
  - Use bios and sign on Passwords.
  - Enable document encryption.
- **Public Wireless Connections**
  - **Be aware of Evil Twin Access Points** that look like the friendly access point that you are trying to utilize in such Wi-Fi Hot Spots as in airports, cafes, hotels and libraries. The rogue access point can be used to "sniff" or "eavesdrop" on wireless communications.
  - Keep software updated.
  - Enable Operating Systems and other software firewalls.
  - Enable encryption which prevents "sniffing". Browser sniffing is a common technique used in websites and web applications in order to determine the web browser a visitor is using. "Sniffing" is a form of wire-tap applied to computer networks. This means that traffic on a segment passes by all hosts attached to that segment. Filters on the network prevent the host machine from seeing traffic addressed to other stations. Sniffing programs turn off the filter, and thus hackers can see everyone's traffic.
  - **Never**
    - *Send confidential info by e-mail*
    - *Send user Id's or passwords*
    - *View online bank statements*
- **Computer Hard Drives**
  - **Do Not** discard old hard drives in the trash without first:
    - *Using specialized disk wiping software to clear data from the hard drive, or better*
    - *Destroy the hard drive if no longer needed.*

WHAT TO DO IF YOU BECOME A VICTIM OF IDENTITY THEFT

IMMEDIATELY!

- Call the Police
  - Go to your local precinct or call to have a police officer come to your home. (631) 852-COPS (2677)
  - Providing the credit reporting agencies with a copy of your police report will allow them to extend the fraud alert on your information to seven years. Contact the three (3) major Credit Reporting Bureaus.
  - Place a fraud alert on your Credit Bureau information.
  - Request your credit bureau reports.
  - Check your reports carefully, make sure you can identify every entry reported, close any accounts you did not open or authorize.
  - The Resource Page contains information on the three (3) major Credit Reporting Agencies.
- Call the creditors involved.
  - Advise them that you are the victim of Identity Theft.
  - Close the affected accounts.
- Correct the address for any mailings in your name being sent to the wrong location by contacting the U.S. Postal Inspection Service (See the enclosed Resource Page for information on the U.S. Postal Inspection Service.).
- Contact the Federal Trade Commission Identity Theft Hotline (See the enclosed Resource Page for information on the Federal Trade Commission.)
- Consider placing a "Security Freeze" on your Credit Bureau Information. See the Resource Page for more information.

Social Security Number Fraud

If you believe someone has been using your social security number to obtain benefits or employment you should also report your complaint to the Social Security Administration. (See the Resource Page for information on the Social Security Administration.)

Internal Revenue Service Fraud

If you believe that you have been the victim of fraudulent filing of documents with the Department of Treasury Internal Revenue Service please report your complaint to the Internal Revenue Service. (See the enclosed Resource Page for information on contacting the Department of Treasury – Internal Revenue Service.)

Take Control!

Here are a few guidelines to regain control of your life and your financial well being by proving to financial institutions that you are the victim and not the perpetrator.

- Gather all the information you possess regarding the theft and use of your personal identifiers.
- Chart a timeline as to the sequence of events as you understand them. Correct the timeline as you gather more information.
- Keep a diary and document phone calls regarding your problem; record the date, time and the names of persons you called and what information was discussed. Get direct phone numbers of those contacted as well as addresses for future correspondence. Refer to the New York State Consumer Protection Website for a sample diary. The website information is on the enclosed Resource Page for your convenience.

- Follow up all phone conversations with a written correspondence confirming the details of your conversation. Send all correspondence certified mail with a return receipt through the U.S. Postal Service.
- Keep hard copies as well as computer copies of all correspondence, bills and charges either sent or received.
- Keep track of expenses related to correcting your personal identifiers or credit information for the possibility of future restitution. Refer to the New York State Consumer Protection Website for information about victim restitution. The website information is on the Resource Page for your convenience.
- Stay organized, that may be difficult in such stressful circumstances so you may need to enlist a family member or close friend to assist you in the effort.

THE SECURITY FREEZE

Identity Theft, when someone uses your name or personal information to open an unauthorized new account or borrow money, or make unauthorized charges, continues to be the most common consumer fraud complaint, affecting approximately 8 to 15 million Americans each year. It is of particular concern in New York, which has the sixth highest per-capita incidence of Identity Theft in the country. New Yorkers have a weapon to use against Identity Theft: the New York State Security Freeze Law.

How a Security Freeze works
At your request, a Security Freeze is placed on your credit file, which is sometimes called your "credit history". The Security Freeze prevents lenders and others from gaining access to your credit report for review. With a Security Freeze in place, the lender will not be able to get a copy of your credit history and, as a result, most lenders will refuse to open a new credit account. The Security Freeze will, in most cases, block someone from opening a new account or borrowing money using your name or personal information. There is no charge for New York State residents, to place a Security Freeze on their credit report if they are the victim of Identity Theft or they are making this request for the first time.

Benefits and risks of a Security Freeze
Not everyone will want to place a Security Freeze on their credit file. With a Security Freeze in place, you won't be able to borrow money, obtain instant credit or get a new credit card until you temporarily lift or permanently remove the Security Freeze. The same is true of new insurance coverage and background checks that might be required by a new employer. Additionally, it can impede renting an apartment or other housing.

How to obtain a Security Freeze
To obtain a Security Freeze, contact each of the three (3) major credit reporting agencies (CRA): TransUnion, Experian and Equifax. By law, the three credit bureaus will have three (3) business days from the date they receive your request to place a Security Freeze on your credit file (in 2010 it decreases to one (1) business day). Additionally, each CRA is required to have a secure website and a dedicated toll-free number to place a Security Freeze. Requests for a Security Freeze must contain personal information that will be specified by each credit bureau. This information may include your name, addresses during the past five years and Social Security number. Credit bureaus need this information to verify your identity and process your request. If you wish to use the mail and write a letter, the Consumer Protection Board's (CPB) website (nysconsumer.gov) contains information on the requirements of each credit bureau, along with sample letters that can be used to initiate our request for a Security Freeze. Each letter must be sent with confirmation of delivery.

What happens next?
The credit bureaus (all of which are private companies) will write back to you within five (5) business days of placing the freeze, confirming that it has been activated. These letters will also contain a password or a Personal Identification Number (PIN). When you want to temporarily lift or permanently remove your Security Freeze, you will use this password or PIN to identify yourself when calling the credit bureaus. Each reporting agency will give you a different password or identification number. The PIN cannot be a Social Security number or a sequential portion thereof.

How to remove the Security Freeze
Consumers may request that the Security Freeze be lifted temporarily, or permanently on their credit report, and should follow the instructions provided by each credit reporting agency. To obtain a temporary lift of the Security Freeze, consumers must inform the credit reporting agency of the name of the party to whom the report should be made available or the period of time when the report should be available to all requestors. Requests for a temporary or a permanent removal of the Security Freeze must be accompanied by proper identification and payment of the applicable fee. Credit reporting agencies must comply with such requests within three (3) business days of receipt. As of September 1, 2009, credit reporting agencies must comply with this request within 15 minutes of the request being received by telephone or secure electronic mechanism (e.g., Internet).

Fees associated with the Security Freeze
You can be charged up to $5 to place a second or subsequent freeze on your report or to remove the Security Freeze. **If you are a victim of Identity Theft, there is no charge for restoring a Security Freeze as long as you provide a copy of an ID theft report from a law enforcement agency or an ID Theft Victim Affidavit from the Federal Trade Commission.**

FREQUENTLY ASKED QUESTIONS

Can I order my own credit report if my file is frozen?
Yes. To obtain a free copy of your credit report (a copy is available from each of the three (3) credit bureaus every twelve (12) months). (See the Resource Page for information on obtaining the free annual credit report.)

Can some companies still review my credit history even with a Security Freeze in place?
Yes. Some private companies, government agencies and courts can still access your credit files with a Security Freeze in place. These include companies with which you're currently doing business; companies to which you owe money; and collection agencies. Credit card companies and other lenders can also access this information in order to offer you credit cards and related services. You have the option of “opting-out” for five (5) years or permanently. “Opting-out” only affects credit offers that use the reporting agencies for information. (See the Resource Page for information on the Opt Out options.)

Will a Security Freeze lower my credit score?
No.

Does one Security Freeze cover everyone in my household?
No. All adults have to freeze their separate credit files, via separate letters requesting the freeze, in order to obtain the benefit of a Security Freeze.

What is the difference between a Security Freeze and Fraud Alert?
A fraud alert is a special message on the credit report that a credit issuer receives when checking a consumer’s credit rating. It tells the credit issuer that there may be fraud involved in the account. It does not limit access to your file. A fraud alert can help protect you against identity theft, but it can also slow down your ability to get new credit. It should not stop you from using your existing credit cards or other accounts. A Security Freeze means that your credit file cannot

be accessed by potential creditors, insurance companies, or employers doing background checks - unless you give your personal consent or authorization.

Where can I obtain more information regarding Identity Theft?
The NYS Consumer Protection Board has prepared information on how to avoid becoming a victim of Identity Theft and what to do if your identity is stolen. That information is available at www.nysconsumer.gov, under "Publications".

For your convenience we have enclosed sample security freeze letters specific to each of the three (3) credit reporting agencies. They are located after the Resource Page.

See the Resource Page for the telephone numbers, online website addresses and location addresses of the three credit reporting agencies.

THE IDENTITY THEFT AFFIDAVIT

To make certain that you do not become responsible for any debts incurred by an identity thief, you must prove to each of the companies where accounts were opened in your name that you didn't create the debt. The ID Theft Affidavit was developed by a group of credit grantors, consumer advocates, and attorneys at the Federal Trade Commission (FTC) for this purpose. Importantly, this affidavit is only for use where a new account was opened in your name. If someone made unauthorized charges to any existing account, call the company for instructions.

While many companies accept this affidavit, others require that you submit more or different forms. Contact each company to find out if they accept it. If they do not accept the ID Theft Affidavit, ask them what information and/or documentation they require.

You may not need the ID Theft Affidavit to absolve you of debt resulting from identity theft if you obtain an Identity Theft Report. We suggest you consider obtaining an Identity Theft Report (Police Report) where a new account was opened in your name. An Identity Theft Report can be used to (1) permanently block fraudulent information from appearing on your credit report; (2) ensure that debts do not reappear on your credit reports; (3) prevent a company from continuing to collect debts or selling the debt to others for collection; and (4) obtain an extended fraud alert.

The ID Theft Affidavit may be required by a company in order for you to obtain applications or other transaction records related to the theft of your identity. These records may help you prove that you are a victim. For example, you may be able to show that the signature on an application is not yours. These documents also may contain information about the identity thief that is valuable to law enforcement. Complete this affidavit as soon as possible. Many creditors ask that you send it within two weeks.

This affidavit has two parts:

- Part One – The ID Theft Affidavit – is where you report general information about yourself and the theft.
- Part Two – The Fraudulent Account Statement - is where you describe the fraudulent account(s) opened in your name. Use a separate Fraudulent Account Statement for each company you need to write to.

When you send the affidavit to the companies, attach **COPIES (NOT ORIGINALS)** of any supporting documents (for example, driver's license or police report). When you have finished completing the affidavit, mail a copy to each creditor, bank, or company that provided the thief with the unauthorized credit, goods, or services you describe. Attach a copy of the Fraudulent Account Statement with information only on accounts opened at the institution to which you are sending the packet, as well as any other supporting documentation you are able to provide. Send the appropriate documents to each company by certified mail, return receipt requested, so you

can prove that it was received. The companies will review your claim and send you a written response telling you the outcome of their investigation. Keep a copy of everything you submit. If you are unable to complete the affidavit, a legal guardian or someone with power of attorney may complete it for you.

For your convenience we have enclosed two (2) sample dispute letters. One is for a newly opened account in your name; the other is for an existing account that has been compromised.

Name:_____**Suffolk County P.D. Central Complaint #:**_____

VICTIM INFORMATION

1. My full legal name is
   _____
   (First) (Middle) (Last) (Jr., Sr., III)

2. (If different from above) When the events described in this affidavit took place, I was known as:
   _____
   (First) (Middle) (Last) (Jr., Sr., III)

3. My date of birth is: _____
   (Day/Month/Year)

4. My Social Security Number is: _____ - ___ - _____

5. My driver's license or identification card state and number is:
   _____

6. My current address is:
   _____
   City: _____ State: _____ Zip Code: _____

7. I have lived at this address since: _____
   (Month/Year)

8. (If different from above) When the events described in this affidavit took place, my address was:
   _____
   City: _____ State: _____ Zip Code: _____

9. I lived at the address in Item 8 from _____ to _____
   (Month/Year) (Month/Year)

10. My daytime telephone number is: (___) ____-_____
    My evening telephone number is: (___) ____-_____

HOW THE FRAUD OCCURRED

CHECK ALL THAT APPLY FOR ITEMS 11 - 17

11. __ I did not authorize anyone to use my name or personal information to seek the money, credit, loans, goods or services described in this report.

Name:_____**Suffolk County P.D. Central Complaint #:**_____

12. __ I did not receive any benefit, money, goods or services as a result of the events described in this report.

13. __ My identification documents (for example, credit cards; birth certificates; driver's license; Social Security Card, etc) were:
____stolen ____lost on or about _____
(day/month/year)

14. __ To the best of my knowledge and belief, the following person(s) used my information, (for example, my name, address, date of birth, existing account numbers, Social Security Number, mother's maiden name, etc.) or identification documents to get money, credit, loans, goods or services without my knowledge or authorization:

_____	_____
Name (If known)	Name (If known)
_____	_____
Address (If known)	Address (If known)
_____	_____
Phone Number(s) (If known)	Phone Number(s) (If known)
_____	_____
Additional Information	Additional Information

15. __ I do NOT know who used my information or identification documents to get money, credit, loans, goods or services without my knowledge or authorization

16. Additional comments: (For example, description of the fraud, which documents or information were used or how the identity thief gained access to your information)

Attach additional pages as necessary

Name:_____**Suffolk County P.D. Central Complaint #:**_____

VICTIM'S LAW ENFORCEMENT ACTIONS

17. (Check only one)
__ I am __ I am **not** willing to assist in the prosecution of the person(s) who committed this fraud.

18. (Check only one)
__ I am __ I am **not** authorizing the release of this information to law enforcement for the purposes of assisting them in the investigation and prosecution of the person(s) who committed this fraud.

19. (Check all that apply): I __ have __ have not reported the events described in this affidavit to the police or other law enforcement agency. The police __ did __ did not write a report. *In the event you have contacted the police or other law enforcement agency please complete the following information:*

Agency #1	Officer/Agency personnel taking report
Date of Report	Report Number (if any)
Phone Number	Email Address (if any)
Agency #2	Officer/Agency personnel taking report
Date of Report	Report Number (if any)
Phone Number	Email Address (if any)

DOCUMENTATION CHECK LIST

Please indicate the supporting documentation you are able to provide to the companies you plan to notify. Attach copies (NOT originals) to the affidavit before sending it to the companies.

20. __ A copy of a valid government-issued photo-identification card (for example, your driver's license, state-issued ID card, or your passport.) If you are under 16 and don't have a photo-ID, you may submit a copy of your birth certificate or a copy of your official school records showing your enrollment and place of residence.

21. __ Proof of residency during the time the disputed bill occurred, the loan was made or the other event took place (for example, a rental/lease agreement in your name, a copy of a utility bill or a copy of an insurance bill).

22. __ A copy of the report filed with the police or sheriff's department. If you are unable to obtain a report or a report number from the police, please indicate that in Item 19. Some companies only need the report number, not a copy of the report. You may want to check with each company.

Name:_____**Suffolk County P.D. Central Complaint #:**_____

SIGNATURE

I certify that, to the best of my knowledge and belief, all the information on and attached to this affidavit is true, correct, and complete and made in good faith. I also understand this affidavit or the information it contains may be made available to federal, state, and/or local law enforcement agencies for such action within their jurisdiction as they deem appropriate. I understand that knowingly making any false or fraudulent statement or representation to the government may constitute a violation of 18 U.S.C. 1001 or other federal, state or local criminal statutes, and may result in imposition of a fine or imprisonment or both.

_____ _____
Signature Date Signed

_____
Notary

Check with each company. Creditors sometimes require notarization. If they do not, please have one witness (non-relative) sign below that you completed and signed this affidavit.

Witness:

_____ _____
Signature Printed Name

_____ _____
Date Telephone Number

Name:_____**Suffolk County P.D. Central Complaint #:**_____

FRAUDULENT ACCOUNT STATEMENT

Completing the Statement

- Make as many copies of this page as you need. Complete a separate page for each company you're notifying and only send it to that company. Include a copy of your signed affidavit.
- List only the account(s) you're disputing with the company receiving this form. See the example below.
- If a collection agency sent you a statement, letter or notice about the fraudulent account, attach a copy of that document (Not the original).

I declare (check all that apply):

__ As a result of the event(s) described in the ID Theft Affidavit, the following account(s) was/were opened at your company in my name without my knowledge, permission or authorization using my personal information or identifying documents.

Creditor Name/Address (The company that opened the account or provided the goods or services)	Account Number	Type of unauthorized Credit/Goods/Services Provided by Creditor (If known)	Date Issued or Opened (If known)	Amount/Value Provided (The amount charged or the cost of the good or services)
Example Example National Bank 22 Main Street Columbus, OH 22722	01234567-89	Auto Loan	01/05/2002	$25.500.00

__ During the time of the accounts described above, I had the following account open with your company:

Billing Name: _____
Billing Address: _____
Account Number: _____

Security Freeze (Sample) letter request to Equifax, Inc.

Note: If this is your first time placing a security freeze, there is no fee for requesting a Security Freeze. Once you remove or temporarily lift the Security Freeze, you will be charged up to $5 to restore the Security Freeze. There is an exception, however, if you are the victim of Identity Theft. You will not be charged this fee if you submit a copy of the police report or a signed copy of a Federal Trade Commission ID Theft Victim Affidavit.

You must send this letter to Equifax by either certified mail or overnight mail through the U.S. Postal Service to:

Equifax Security Freeze
PO Box 105788
Atlanta, GA 30348

Date:

Dear Equifax:

I would like to place a security freeze on my credit file.

My full name (with middle initial and generation, such as Jr. or Sr.) is:

My complete current address is:

My date of birth is:

My Social Security number is:

I am also enclosing a copy of a document (such as a utility bill) that verifies my current mailing address.

Yours truly,

Security Freeze (Sample) Request to Experian Inc.

Information on what to send to Experian:
Make sure that each copy of your personal information is legible (enlarge if necessary) and it displays your name and current mailing address, as well as the date of when the document was issued. The date(s) on these documents must be recent. Experian will NOT accept credit card statements, voided checks, lease agreements, magazine subscriptions or postal service forwarding orders such as proof.

To protect your personal information, Experian does not return correspondence sent to them. So keep your original documents and only send copies to Experian.

Note: If this is your first time placing a security freeze, there is no fee for requesting a Security Freeze. Once you remove or temporarily lift the Security Freeze, you will be charged up to $5 to restore the Security Freeze. There is an exception, however, if you are the victim of Identity Theft. You will not be charged this fee if you submit a copy of the police report or a signed copy of a Federal Trade Commission ID Theft Victim Affidavit.

You must send this letter to Experian by either certified mail or overnight mail through the U.S. Postal Service to:

Experian Security Freeze
PO Box 9554
Allen, TX 75013

Date:

Dear Experian:

I would like to place a security freeze on my credit file.

My full name (with middle initial and generation, such as Jr. or Sr.) is:

My Social Security number is:

My date of birth is:

My complete current address is:
Below is a list of my addresses for the past two years:

I am enclosing one copy of a government-issued identification card, such as a driver's license, state ID card, military ID card, etc.

To help verify my current address, I am also enclosing one copy of a utility bill, bank or insurance statement, etc.

Yours truly,

Security Freeze (Sample) Request to TransUnion Inc.

Note: If this is your first time placing a security freeze, there is no fee for requesting a Security Freeze. Once you remove or temporarily lift the Security Freeze, you will be charged up to $5 to restore the Security Freeze. There is an exception, however, if you are the victim of Identity Theft. You will not be charged this fee if you submit a copy of the police report or a signed copy of a Federal Trade Commission ID Theft Victim Affidavit.

TransUnion reserves the right to ask for further proof of identity should the information you provide not be complete or if security warrants it. The following can be used as proof of address and Social Security number: copies of current driver's license, bank or credit union statement, Medicaid or Medicare card, paycheck stub, state ID card, W2 form.

TransUnion will accept letters by regular mail, certified mail or overnight mail from the U.S. Postal Service at this address:

TransUnion
Fraud Victim Assistance Department
PO Box 6790
Fullerton, CA 92834

Date:

Dear TransUnion;

I would like to place a security freeze on my credit file.

My name is:

Other name(s) used:

My current address is:

My previous address is (if you have other addresses in the previous five (5) years):

My home phone is:

My Social Security number is:

My date of birth is:

My driver's license # is:

Yours truly,

Sample Dispute Letter

Date
Your Name
Your Address
Your City, State, Zip Code

Complaint Department
Company Name
Address
City, State, Zip Code

Dear Sir or Madam:

I am writing to dispute the following information in my file. I have circled the items I am disputing on the attached copy of the report I received.

This item *(identify the item(s) disputed by name of source, such as creditors or tax court, and identify type of item, such as credit account, judgment, etc.)* is *(inaccurate or incomplete)* because *(describe what is inaccurate or incomplete and why)*. I am requesting that the item be removed *(or request another specific change)* to correct the information.

Enclosed are copies of *(use this sentence if applicable and describe any enclosed documentation, such as a police report, Identity Theft Affidavit, payment records, court documents)* supporting my position. Please reinvestigate this *(these)* matter(s) and *(delete or correct)* the disputed item(s) as soon as possible.

In addition, pursuant to FACTA Public Law 108, as a victim of identity theft, I am requesting that you provide me with copies of any and all applications and business transaction records related to the fraudulent account(s). The copies of the records can be (mailed to me at the above address or faxed to me at this telephone number: (xxx) xxx-xxxx). **In addition, please make these records available to the Suffolk County Police Department upon their request.**

Sincerely,

Your name.

Enclosures *(list below what is enclosed)*

Sample Dispute Letter for Existing Accounts

Date
Your Name
Your Address
Your City, State, Zip Code
Your Account Number

Name of Creditor
Billing Inquiries
Address
City, State, Zip Code

Dear Sir or Madam:

I am writing to dispute a fraudulent *(charge or debit)* on my account in the amount of $_____. I am a victim of identity theft, and I did not make this *(charge or debit).* I am requesting that the *(charge be removed or the debit be reinstated)*, that any finance and/or other charges related to the fraudulent amount be credited, as well, and that I receive an accurate statement.

Enclosed are copies of *(use this statement to described any enclosed information, such as a police report or ID Theft Affidavit)* supporting my position. Please investigate this matter and correct the fraudulent *(charge or debit)* as soon as possible.

In addition, pursuant to FACTA Public Law 108, as a victim of identity theft, I am requesting that you provide me with copies of any and all applications and business transaction records related to the fraudulent account(s). The copies of the records can be *(mailed to me at the above address or faxed to this telephone number: (xxx) xxx-xxxx)*. **In addition, please make these records available to the Suffolk County Police Department upon their request.**

Sincerely,

Your Name

Enclosures *(list below what is enclosed)*

FAIR AND ACCURATE CREDIT TRANSACTIONS ACT OF 2003
PUBLIC LAW 108-159, DECEMBER 4, 2003

SEC. 151. SUMMARY OF RIGHTS OF IDENTITY THEFT VICTIMS

a) IN GENERAL –
   1) SUMMARY - Section 609 of the Fair Credit Reporting Act (15 U.S.C. 1681g) is amended by adding at the end of the following:
      d) SUMMARY OF RIGHTS OF IDENTITY THEFT VICTIMS –
         1) IN GENERAL - The Commission, in consultation with the Federal banking agencies and the National Credit Union Administration, shall prepare a model summary of the rights of consumers under this title with respect to the procedures for remedying the effects of fraud or identity theft involving credit, an electronic fund transfer, or an account or transaction at or with a financial institution or other creditor.
         2) SUMMARY OF RIGHTS AND CONTACT INFORMATION - Beginning 60 days after the date on which the model summary of rights is prescribed in final form by the Commission pursuant to paragraph 1), if any consumer contacts a consumer reporting agency and expresses a belief that the consumer is a victim of fraud or identity theft involving credit, an electronic fund transfer, or an account or transaction at or with a financial institution or other creditor, the consumer reporting agency shall, in addition to any other action that the agency may take, provide the consumer with a summary of rights that contains all of the information required by the Commission under paragraph 1), and information on how to contact the Commission to obtain more detailed information.
      e) INFORMATION AVAILABLE TO VICTIMS –
         1) IN GENERAL - For the purpose of documenting fraudulent transactions resulting from identity theft, not later than 30 days after the date of receipt of a request from a victim in accordance with paragraph 3), and subject to verification of the identity of the victim and the claim of identity theft in accordance with paragraph 2) <u>a business entity that has provided credit to, provided for consideration products, goods, or services to, accepted payment from, or otherwise entered into a commercial transaction for consideration with, a person who has allegedly made unauthorized use of the means of identification of the victim, shall provide a copy of application and business identification of the victim, shall provide a copy of application and business transaction records in the control of the business entity, whether maintained by the business entity or by another person on behalf of the business entity, evidencing any transaction alleged to be a result of identity theft to –</u>
            a. The victim
            b. Any Federal, State or Local government law enforcement agency or officer specified by the victim in such a request; or
            c. Any law enforcement agency investigating the identity theft and authorized by the victim to take receipt of records provided under this subsection.
         2) VERIFICATION OF IDENTITY AND CLAIM - Before a business entity provides any information under paragraph 1), unless the business entity, at its discretion, otherwise has a high degree of confidence that it knows the identity of the victim making a request under paragraph 1), the victim shall provide to the business entity –

a. as proof of positive identification of the victim, at the election of the business entity—

i). the presentation of a government-issued identification card;

ii). personally identifying information of the same type as was provided to the business entity by the unauthorized person; or

iii). Personally identifying information that the business entity typically requests from new applicants or for new transactions at the time of the victim's request for information, including any documentation described in clauses i) and ii); and

b. as proof of a claim of identity theft, at the election of the business entity –

i). A copy of a police report evidencing the claim of the victim of identity theft; and

ii). a properly completed –

I. copy of a standardized affidavit of identity theft developed and made available by the Commission; or

II. an affidavit of fact that is acceptable to the business entity for that purpose.

3). PROCEDURES – The request of a victim under paragraph 1) shall –

a. be in writing

b. be mailed to an address specified by the business entity, if any; and

c. if asked by the business entity, include relevant information about any transaction alleged to be a result of identity theft to facilitate compliance with this section including –

i. if known by the victim (or if readily obtainable by the victim), the date of the application or transaction; and

ii. if known by the victim (or if readily obtainable by the victim), any other identifying information such as an account or transaction number

4). NO CHARGE TO VICTM – Information required to be provided under paragraph 1) shall be so provided without charge.

5). AUTHORITY TO DECLINE TO PROVIDE INFORMATION – A business entity may decline to provide information under paragraph 1) if, in the exercise of good faith, the business entity determines that –

this subsection does not require disclosure of this information;

a. after reviewing the information provided pursuant to paragraph 2), the business entity does not have a high degree of confidence in knowing the true identity of the individual requesting the information;

b. the request for the information is based on a misrepresentation of fact by the individual requesting the information relevant to the request for information; or

c. the information requested is Internet navigational data or similar information about a person's visit to a website or online service.