East Hampton Police Department

20 East High Street, East Hampton, CT 06424
(860) 267-9544 / (860) 267-9922

Identity Theft Victim's Packet

Information and Instructions

This packet is to be completed once you have contacted the East Hampton Police Department and obtained a Police case report number related to your identity theft case. To obtain a Police case report number, call 860-267-9544. Please keep track of your report number as creditors, financial institutions and credit reporting agencies will ask for it.

My East Hampton Police Department Case Report Number is:

Case #_____

This packet contains information to assist you in the correction of your credit and to help ensure that you are not responsible for the debts incurred by the identity thief.
In addition, this packet includes information that will allow you to obtain financial records related to the fraudulent accounts and provide those records to law enforcement, without which we cannot conduct an investigation for prosecution.
We recognize that some victims are only interested in the correction of their credit and do not necessarily wish for prosecution; therefore, we request that you only submit this packet to the East Hampton Police Department if you desire prosecution. *It is important to understand that in the event that a suspect is identified and arrested and the case proceeds to court, you as the victim would mostly likely be required to appear and testify in court.*

In identity theft cases, it is difficult to identify the suspect(s) as they often use inaccurate information such as addresses and phone numbers. Frequently the investigator cannot find evidence to prove who actually used the victim's name and/or personal information over the phone or internet. Often, the cell phones that identity thieves use are nontraceable prepaid phones or opened with fraudulent information. Completion of dispute letters will provide us with necessary documentation that is required for prosecution. Examples of the document evidence we need to investigate your case are included in this packet. It is important to note that even if the suspect cannot be identified for prosecution, it will not affect your ability to correct the fraudulent accounts and remove them from your credit report. Furthermore, when you report your identity crime to the East Hampton Police Department, all of the relevant information from your case is entered into our database which will allow us to cross-reference your report with potential suspects who are involved in or arrested on other cases.

Helpful Hints:

• Remember that each creditor has different policies and procedures for correcting fraudulent accounts

• Do not provide originals and be sure to keep copies of everything you provide to the creditors or companies involved in the identity theft.

• Write down all dates, times and the names of individuals you speak to regarding the identity theft and correction of your credit.

Step 1: Contact your bank and other credit card issuers.

If the theft involved **existing bank accounts** (checking or savings accounts as well as credit or debit card) you should do the following:

• Close the account that was used fraudulently or put stop payments on all outstanding checks that might have been written without your knowledge.

• Close all credit card accounts that were used fraudulently.

• Close any account accessible by debit card if it has been accessed fraudulently.

• Open up new accounts protected with a secret password or personal identification number (PIN)

If the identity theft involved the creation of **new bank accounts,** you should do the following:

• Call the involved financial institution and notify them of the identity theft.

• They will likely require additional notification in writing. (see step 4)

Step 2: Contact all three (3) major credit reporting bureaus.

First request the credit bureaus place a **"Fraud Alert"** on your file. A fraud alert will put a notice on your credit report that you have been the victim of identity theft. Merchants and financial institutions **may** opt to contact you directly before any new credit is taken out in your name. *Some states allow for a Security Freeze in which a PIN can be designated on your credit file and subsequently the PIN must then be given in order for credit to be extended*. Connecticut currently participates in this program.

Fraud Alerts : There are two types of fraud alerts: an initial alert, and an extended alert.

An initial alert stays on your credit report for at least 90 days. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial alert is appropriate if your wallet has been stolen or if you've been taken in by a "phishing" scam. When you place an initial fraud alert on your credit report, you're entitled to one free credit report from each of the three nationwide consumer reporting companies.

An extended alert stays on your credit report for seven years. You can have an extended alert placed on your credit report if you've been a victim of identity theft and you provide the consumer reporting company with an "identity theft report." When you place an extended alert on your credit report, you're entitled to two free credit reports within twelve months from each of the three nationwide consumer reporting companies. In addition, the consumer reporting companies will remove your name from marketing lists for pre-screened credit offers for five years unless you ask them to put your name back on the list before then.

The following is a list of the three (3) major credit reporting bureaus for victims to report fraud:

Equifax TransUnion Experian

Consumer Fraud Division Fraud Victim Assistance Dept Nat. Consumer Assist

800-525-6285 800-680-7289 888-397-3742

P.O. Box 740256 P.O. Box 6790 P.O. Box 9530

Atlanta, GA 30374 Fullerton, CA 92834 Allen, TX 75013

Step 3: File a report with the Federal Trade Commission.

You can go on-line to file an identity theft complaint with the FTC at www.FTC.gov and click on the ID Theft icon or by calling 1-877-IDTHEFT. **Print a copy of your filed complaint for inclusion in this packet .**

Step 4: Contact creditors involved in the Identity Theft by phone and in writing.

This step involves contacting all the companies or institutions that provided credit or opened new accounts for the suspect or suspects. Some examples include banks, mortgage companies, utility companies, telephone companies, cell phone companies, etc**.**

Provide the creditors with the completed Identity Theft Affidavit (some may require that you use their own affidavit), Letter of Dispute, and a copy of the FACTA Law.

FTC Identity Theft Affidavit

A copy of the FTC Identity Theft Affidavit can be found at the end of this packet. This is the same affidavit that the FTC makes available to victims of identity theft. The affidavit requests information regarding you as the victim, how the fraud occurred, law enforcement's actions, documentation checklist and Fraudulent Account Statement. NOTE. Some creditors, financial institutions, or collection agencies have their own affidavit that you may have to complete.

Letters of Dispute

Sample copies of the Letters of Dispute can also be found at the end of this packet. **This letter needs to be completed for every creditor involved in the identity theft.** The letter of dispute should contain information related to the fraudulent account(s), your dispute of the account(s), and your request for the information to be corrected. **In addition, the letter should reference FACTA and make a request for copies of any and all records related to the fraudulent accounts be provided to you and made available to the East Hampton Police Department**.

FACTA Law

A portion of the FACTA Law can also be found at the end of this packet. As previously discussed in this packet, FACTA allows for you to obtain copies of any and all records related to the fraudulent accounts. **You are then permitted to provide law enforcement with copies of the records you received related to the fraudulent accounts; thereby allowing us to bypass the sometimes difficult process of obtaining search warrants for the very same information**. **It also allows you to request the information be made available to the East Hampton Police Department.** We have found it useful to provide a copy of the FACTA Law with the submission of the Identity Theft Affidavit and Letter of Dispute to the individual creditors.

Step 5: Submit the Identity Theft Affidavit AND copies of all information and records obtained from the creditors with regard to the fraudulent accounts to:

East Hampton Police Department
20 East High Street,
East Hampton , CT 06424
860-267-9544

We request that you only submit this packet to the East Hampton Police Department if you desire prosecution and would be willing and available to appear and testify in court should a suspect be identified and arrested.

If you decide to submit the packet, please call the Police Department at 860-267-9544 and speak with an Investigator before doing so to ensure that your packet is complete and contains the necessary document evidence. We request that you submit everything at once. The types of document evidence needed are listed on the next page. Be sure to write your police report number on all items submitted.

After review, an Investigator will speak with you about your case. Frequently the investigator cannot find evidence to prove who actually used the victim's name and/or personal information over the phone or internet.

It is important to note that even if the suspect cannot be identified for prosecution, it will not affect your ability to correct the fraudulent accounts and remove them from your credit report.

Additional Useful Information :

www.ftc.gov/bcp/edu/microsites/idtheft – provides information related to identity theft.

Other entities you may want to report your identity theft to:

- ***Post Office –*** *If you suspect that your mail has been stolen or diverted with a false change-of-address request, contact your local postal inspector. You can obtain the address and telephone number of the postal inspector for your area at United States Postal Service website: www.usps.com/ncsc/locators/findis.html or by calling 800-275-8777.*
- ***Social Security Administration –*** *If you suspect that someone is using your social security number to obtain employment, contact the Social Security Administration's fraud hotline at 1-800-269-0271. Order a copy of your Personal Earnings and Benefit Estimate Statement (PEBES) to check the accuracy of your work history on file with the Social Security Administration. You can obtain a PEBES application at your local Social Security office or at http://www.ssa.gov/online/ssa-7004.pdf .*
- ***State Department –*** *If your passport has been stolen, notify the passport office in writing. You can obtain additional information from the State Department's website: http://travel.state.gov/reportppt.html .*
- ***If you are contacted by a collection agency*** *- about a debt for which you are not responsible, immediately notify them that you did not create the debt and that you are a victim of identity theft. Follow up with the collection agency and creditor in writing and include a copy of your police report, ID Theft Affidavit, Letter of Dispute and a copy of the FACTA Law.*

What is identity theft?

Identity theft occurs when someone uses your personally identifying information, like your name, Social Security number, or credit card number, without your permission, to commit fraud or other crimes. The Federal Trade Commission estimates that as many as 9 million Americans have their identities stolen each year. In fact, you or someone you know may have experienced some form of identity theft. The crime takes many forms. Identity thieves may rent an apartment, obtain a credit card, or establish a telephone account in your name. You may not find out about the theft until you review your credit report or a credit card statement and notice charges you didn't make—or until you're contacted by a debt collector. Identity theft is serious. While some identity theft victims can resolve their problems quickly, others spend hundreds of dollars and many days repairing damage to their good name and credit record. Some consumers victimized by identity theft may lose out on job opportunities, or be denied loans for education, housing or cars because of negative information on their credit reports. In rare cases, they may even be arrested for crimes they did not commit.

How do thieves steal an identity?

Identity theft starts with the misuse of your personally identifying information such as your name and Social Security number, credit card numbers, or other financial account information. For identity thieves, this information is as good as gold. Skilled identity thieves may use a variety of methods to get hold of your information, including: Dumpster Diving: They rummage through trash looking for bills or other paper with your personal information on it. Skimming: They steal credit/debit card numbers by using a special storage device when processing your card. Phishing: They pretend to be financial institutions or companies and send spam or pop-up messages to get you to reveal your personal information. Changing Your Address: They divert your billing statements to another location by completing a change of address form. Old-Fashioned Stealing: They steal wallets and purses; mail, including bank and credit card statements; pre-approved credit offers; and new checks or tax information. They steal personnel records, or bribe employees who have access. Pretexting: They use false pretenses to obtain your personal information from financial institutions, telephone companies, and other sources.

What do thieves do with a stolen identity?

Once they have your personal information, identity thieves use it in a variety of ways. Credit card fraud: They may open new credit card accounts in your name. When they use the cards and don't pay the bills, the delinquent accounts appear on your credit report. They may change the billing address on your credit card so that you no longer receive bills, and then run up charges on your account. Because your bills are

now sent to a different address, it may be some time before you realize there's a problem. Phone or utilities fraud: They may open a new phone or wireless account in your name, or run up charges on your existing account. They may use your name to get utility services like electricity, heating, or cable TV. Bank/finance fraud: They may create counterfeit checks using your name or account number. They may open a bank account in your name and write bad checks. They may clone your ATM or debit card and make electronic withdrawals your name, draining your accounts. They may take out a loan in your name. Government documents fraud: They may get a driver's license or official ID card issued in your name but with their picture. They may use your name and Social Security number to get government benefits. They may file a fraudulent tax return using your information. Other fraud: They may get a job using your Social Security number. They may rent a house or get medical services using your name. They may give your personal information to police during an arrest. If they don't show up for their court date, a warrant for arrest is issued in your name.

How can you find out if your identity was stolen?

The best way to find out is to monitor your accounts and bank statements each month, and check your credit report on a regular basis. If you check your credit report regularly, you may be able to limit the damage caused by identity theft. For more information, visit www.annualcreditreport.com

Documentation for Investigation and Prosecution

The following items of evidence should be obtained by using the sample dispute letters to dispute charges and requesting all documentation related to the account(s).

1. If your existing accounts are being accessed, please obtain the following types documents:

A. Bank statements or bills showing where the transaction occurred

1) Please circle or underline the fraudulent transactions

2) Using a highlighter, make it impossible to read photocopies

3) Please attempt to obtain a physical address fro the transactions from your bank

B. Bills from companies showing merchandise ordered

1) Addresses where items were delivered

2) What phone numbers were associated with the order

C. Any information from the creditor that shows how or where the account was used

D. The name and the phone number of any representatives from the businesses you deal with

2. If new accounts have been opened in your name please obtain the following:

A. Bank statements that you received for accounts that are not yours

B. Credit reports showing the accounts that are not yours

1) Please circle or underline al accounts that are not yours

2) Using a highlighter, make it impossible to read photocopies

C. Bills from utility companies that you did not open

D. Letters or documentation from creditors or utility companies that contain:

1) Copies of applications for credit

2) How the account was opened (i.e. in person, over the phone, on the internet)

3) Where the account was opened if done in person

4) Where the account is being used (i.e. address of transactions)

5) Address where any cards, bills, merchandise or correspondence was mailed

6) Any phone numbers associated with the fraudulent account

E. The name, employee number and phone number of any representatives from the businesses you deal with

3. If someone is using your personal information for employment we will need:

A. Copies of Department of Economic Securities or Social Security Administration report showing your information being used for employment in East Hampton.

B. If only your Social Security Number is being used for employment, please provide a **stamped** Social Security Number verification letter from the Social Security Administration that verifies the Social Security Number in question is assigned to you

If only a partial account number is listed on the document, please write the entire number on the copy you send to us.

INSTRUCTIONS FOR COMPLETING THE ID 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 an existing account, call the company for instructions. While many companies accept this affidavit, others require that you submit more or different forms. Before you send the affidavit, 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 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.

This affidavit has two parts:

· Part One of the ID Theft Affidavit is where you report general information about yourself and the theft.

· Part Two is the Fraudulent Account Statement this 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). Before submitting your affidavit, review the disputed account(s) with family members or friends who may have information about the account(s) or access to them. Complete this affidavit as soon as possible. Many creditors ask that you send it within two weeks. Delays on your part could slow the investigation. Be as accurate and complete as possible. You may choose not to provide some of the information requested. However, incorrect or incomplete information will slow the process of investigating your claim and absolving the debt. Print clearly. 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. Except as noted, the information you provide will be used only by the company to process your affidavit, investigate the events you

report, and help stop further fraud. If this affidavit is requested in a lawsuit, the company might have to provide it to the requesting party. Completing this affidavit does not guarantee that the identity thief will be prosecuted or that the debt will be cleared.

If you haven't already done so, report the fraud to the following organizations:

1. Any one of the nationwide consumer reporting companies to place a fraud alert on your credit report. Fraud alerts can help prevent an identity thief from opening anymore accounts in your name. The company you call is required to contact the other wo, which will place an alert on their versions of your report, too.

. Equifax: 1-800-525-6285; www.equifax.com

. Experian: 1-888-EXPERIAN (397-3742); www.experian.com

. TransUnion: 1-800-680-7289; www.transunion.com

In addition, once you have placed a fraud alert, you're entitled to order one free credit report from each of the three consumer reporting companies, and, if you ask, they will display only the last four digits of your Social Security number on your credit reports.

2. The security or fraud department of each com pany where you know, or believe, accounts have been tampered with or opened fraudulently. Close the accounts. Follow up in writing, and include copies (NOT originals) of supporting documents.

It's important to notify credit card companies and banks in writing.

Send your letters by certified m ail, return receipt requested, so you can document what the company received and when. Keep a file of your correspondence and enclosures. When you open new accounts, use new Personal Identification Numbers (PINs) and passwords. Avoid using easily available information like your m other's maiden name, your birth date, the last four digits of your Social Security number, your phone number, or a series of consecutive numbers.

DO NOT SEND AFFIDAVIT TO THE FTC OR ANY OTHER GOVERNMENT AGENCY

3. Your local police or the police in the community where the identity theft took place. Provide a copy of your ID Theft Complaint filed with the FTC (see below), to be incorporated into the police report. Get a copy of the police report or, at the very least, the number of the report. It can help you deal with creditors who need proof of the crime. If the police are reluctant to take your report, ask to file a .Miscellaneous Incidents Report, or try another jurisdiction, like your state police. You also can check with your state Attorney General's office to find out if state law requires the police to take reports for identity theft. Check the Blue Pages of your telephone directory for the phone number or check www.naag.org for a list of state Attorneys General.

4. The Federal Trade Commission. By sharing your identity theft complaint with the FTC, you will provide important information that can help law enforcement officials across the nation track down identity thieves and stop them. The FTC also can refer victim's complaints to other government agencies and companies for further action, as well as investigate companies for violations of laws that the FTC enforces. You can file a complaint online at www.consumergov/idtheft. If you don't have Internet access, call the FTC's Identity Theft Hotline, toll-free: 1-877-IDTHEFT (438-4338); TTY: 1-866-653-4261; or write: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580. W hen you file an ID Theft Complaint with the FTC online, you will be given the option to print a copy of your ID Theft Complaint. You should bring a copy of the printed ID Theft Complaint with you to the police to be incorporated into your police report. The ID Theft Complaint, in conjunction with the police report, can create an Identity Theft Report that will help you recover m ore quickly. The ID Theft Complaint provides the supporting details necessary for an Identity Theft Report, which go beyond the details of a typical police report.

East Hampton Police Department Case Number: _____

ID Theft Affidavit

My full legal name is _____

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 are_____

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 _____until_____(month/year) (month/year)

10. My daytime telephone number is (____)_____

My evening telephone number is (_____)_____

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.

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

Name _____ East Hampton Police Department Case Number: _____

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 _____ East Hampton Police Department Case Number: _____

17. (check only one)

☐ I am willing to assist in the prosecution of the person(s) who committed this fraud.

☐ I am NOT willing to assist in the prosecution of the person(s) who committed this fraud.

18. (check only one)

☐ I am 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.

☐ 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 not reported the events described in this affidavit to the police or other law enforcement agency.

☐ The police 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)

Please indicate the supporting documentation you are able to provide to the companies you plan 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.

Name _____ East Hampton Police Department Case Number: _____

22. A copy of the report filed with the police or sheriff's department. If you are unable to obtain a report or 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. 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 that 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 the 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 _____ East Hampton Police Department Case Number: _____

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:

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: _____

Sample Dispute Letter

Date
Your Name
Your Address, City, State, Zip Code
Complaint Department
Name of Company
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 dispute on the attached copy of the report I received. This item (identify 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) he disputed item(s) as soon as possible. In addition, pursuant to FACTA..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 address listed below or faxed to the number listed below. **In addition, please take these records available to the East Hampton Police Department upon their request.** Sincerely, Your name
Enclosures: (List what you are enclosing.)

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 reinstated), that any finance and other charges related to the fraudulent amount be credited, as well, and that I receive an accurate statement. Enclosed are copies of (use this sentence to describe any enclosed information, such as a police report or Identity Theft Affidavit) supporting my position. Please investigate this matter and correct the fraudulent (charge or debit) as soon as possible.
In addition, pursuant to…..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 address listed below or faxed to the number listed below).

In addition, please make these records available to the East Hampton Police Department upon their request.

Sincerely,
Your name
Enclosures: (List what you are enclosing.)

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 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), 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 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--`(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 VICTIM- 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-- `(A) this subsection does not require disclosure of the information;`(B) 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; `(C) 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 `(D) the information requested is Internet navigational data or similar information about a person's visit to a website or online service.