WALLINGFORD POLICE DEPARTMENT

135 North Main Street
Wallingford, CT 06492
203-294-2800

IDENTITY THEFT PACKET

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 law enforcement cannot conduct an investigation for prosecution.

This packet contains a summary of some of the steps to take. Please refer to the booklet: "Taking Charge: What to Do If Your Identity is Stolen" which has been issued by the Federal Trade Commission (FTC) and is available at the main desk of police headquarters or visit the FTC website at: www.ftc.gov

Identity theft occurs when somebody steals your personal information (credit/debit card numbers, social security number, etc.) and poses as you, running up charges or emptying your bank accounts. It could take months or years to learn if you are a victim. Some people do not find out until they apply for a loan and get turned down because of a bad credit report.

Some ways to reduce your chance of becoming a victim of this type of crime are:

- Do not give out your personal information! Do not give this information over the telephone or the computer unless you are 100 percent sure of who you are talking to and YOU initiated the contact.
- Destroy unused financial solicitations such as credit card applications and other financial documents that you receive unsolicited through the mail. Tear them up or shred them.
- Report lost or stolen checks, ATM cards, or debit/credit cards immediately.
- Make sure your mailbox is secure and remove mail as soon as possible.
- If you do not receive an expected debit/credit card or other financial statement, contact your financial institution immediately. Thieves may have removed mail from your mailbox.
- Check your credit report at a minimum, annually. This lets you know of any unauthorized access.

In identity theft cases it is difficult to identify the suspect(s) as they often use inaccurate information such as addresses and phone numbers. 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.

Common Scams

Foreign Money	Internet Auctions	Grandparents Phone Scam	Computer Virus Fix
Debt Elimination	Medicare Fraud	Home Improvement	Classified Ads (ie: craigslist, offerup)
IRS Scam			

Step 1: Contact Your Bank and Credit Card Issuers

If the theft involved existing bank accounts (checking or savings accounts as well as credit or debit cards) 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). DO NOT use previous passwords or PINs.

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 Bureau's.

First request the credit bureau's 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. Ask the credit reporting bureau's if your state is participating in the Security Freeze Program.

www.scamsafe.com – provides useful information related to identity theft and indicates which states participate in the Security Freeze Program.

www.annualcreditreport.com – provides one free credit report, per credit bureau agency, per year, with subsequent credit reports available at a nominal fee.

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

EQUIFAX	**EXPERIAN**	**TRANSUNION**
Consumer Fraud Division	Nat. Consumer Assistance	Fraud Victim Assistance Dept.
P.O. Box 740256	P.O. Box 9530	P.O. Box 6790
Atlanta, GA 30374	Allen, TX 75013	Fullerton, CA 92834
1-800-525-6285	1-888-397-3742	1-800-680-7289
www.equifax.com	www.experian.com	www.transunion.com

Step 3: File a Report with the Federal Trade Commission (FTC)

You can go on-line to file an identity theft complaint with the FTC at www.ftc.gov/idtheft or by calling 1-877-IDTHEFT.

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(s). Some examples include banks, mortgage companies, utility companies, telephone companies, cell phone companies, etc.

Letters of Dispute

Sample copies of the Letters of Dispute can be found in the book **"Taking Charge: What To Do If You Identity Is Stolen"** which can be obtained from the main desk at Wallingford Police headquarters. 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 the FACTA Law and make a request for all copies of any and all records related to the fraudulent account(s) be provided to you and made available to the Wallingford Police Department.

Fair and Accurate Credit Transactions Act (FACTA)

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 the law enforcement 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 Wallingford Police Department.

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 the United States Postal Service website: www.usps.com/ncscllocators/findis.html or by calling 1-800-275-8777

- **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 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/passportlost/us/us_848.html

ADDITIONAL USEFUL INFORMATION

- 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 Identity Theft Victim's FACTA Law.

- To report fraudulent use of personal checks, contact the following national checking agencies:

Checkrite	1-800-766-2748
Chexsystems	1-800-428-9623
CrossCheck	1-800-843-0760
Certigy/Equifax	1-800-437-5120
International Check	1-800-526-5380
SCAN	1-800-262-7771
TeleCheck	1-800-710-9898

- Call the ID Theft Clearinghouse at 1-877-IDTHEFT (438-4338) to report the theft. Counselors will take your complaint and advise you on how to deal with the credit related problems that could result from ID theft. The Identity Theft Hotline gives you one place to report the theft to the federal government and receive helpful information.

- For more information, the following (non-profit) websites are great resources on identity theft:

Federal Trade Commission	www.consumer.gov/idtheft
Identity Theft Resource Center	www.idtheftcenter.org
Privacy Rights Clearinghouse	www.privacyrights.org
Social Security Online	www.ssa.gov/pubs/idtheft.htm
U.S. Postal Inspection Service	www.usps.com/postalinspectors

You must file a report with your local police department or the police department where the identity theft took place. Get the report number or a copy of the report in case the bank, credit card company, or others need proof of the crime.

TAX RECORDS

How do you know if your tax records have been affected?

Usually an identity thief uses a legitimate taxpayer's identity to fraudulently file a tax return and claim a refund. Generally, the identity thief will use a stolen Social Security Number (SSN) to file a forged tax return and attempt to get a fraudulent refund early in the filing season.

You may be unaware that this has happened until you file your return later in the filing season and discover that two returns have been filed using the same SSN.

Be alert to possible identity theft if you receive an IRS notice or letter that states:

- More than one tax return for you was filed

- You have a balance due, refund offset, or have had collection actions taken against you for a year you did not file a tax return

- IRS records indicate you received wages from an employer unknown to you

What to do if your tax records were affected by Identity Theft:

If you receive notice from the IRS, respond immediately. If you believe someone may have used your SSN fraudulently, please notify the IRS immediately by responding to the name and number printed on the notice of the letter. You will need to fill out the IRS Identity Theft Affidavit, Form 14039.

For victims of identity theft who have previously been in contact with the IRS and **have not achieved a resolution**, please contact the IRS Identity Protection Specialized Unit at 1-800-908-4490.

How to protect your tax records:

If your tax records are not currently affected by identity theft, but you believe you may be at risk due to a lost/stolen purse or wallet, questionable credit card activity, or credit report, etc., contact the IRS Identity Protection Specialized Unit at 1-800-908-4490.

How you can minimize the chance of becoming a victim:

- Don't carry your social security card or any document(s) with your SSN on it
- Don't give a business your SSN just because they ask. Give it only when required
- Protect your financial information
- Check your credit report every 12 months
- Secure personal information in your home
- Protect your personal computer(s) by using firewalls, anti-spam/virus software, update security patches, and change passwords for Internet accounts
- Don't give personal information over the phone, through the mail, or on the Internet unless you have initiated the contact or you are sure you know who you are dealing with