CITY OF ROCHESTER, MINNESOTA
POLICE DEPARTMENT
101 4TH Street Southeast
Rochester, Minnesota 55904-3761
507-285-8580 • Fax 507-281-7354

To: **Identity Theft and Internet Crime Victims**

From: **Rochester Police Department**

Subject: **Resources and Reporting Procedure on Identity Theft and Internet Related Crimes**

The Rochester Police Department recognizes that victims of Identity Theft may feel confused and overwhelmed by all that is necessary to restore their name and credit after being victimized. This packet is for you to keep and 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 the Rochester Police Department, 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. Where victims don't want to proceed with prosecution there is no need to provide the Rochester Police Department with the required documents and information. **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 most likely be required to appear and testify in court.**

In Identity Theft and Internet related crimes investigators frequently cannot find enough 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.** Furthermore, when you report your identity crime to the Rochester Police Department, all of the relevant information from your case is entered into our records system which will allow us to cross-reference your report with potential suspects who are involved in or arrested on other cases.

The following steps should be taken if you are a victim of Identity Theft or an Internet related crime involving your identity, credit or finances.

Step 1 Contact your bank and other credit card issuers.

If the theft involved **existing bank accounts** (checking, savings, 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 may 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 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.

Step 2 Place a fraud alert on your credit reports, and review your credit reports.

Fraud alerts can help prevent an identity thief from opening any more accounts in your name. Contact the toll-free fraud number of any of the three consumer reporting companies below to place a fraud alert on your credit report. You only need to contact one of the three companies to place an alert. The company you call is required to contact the other two, which will place an alert on their versions of your report as well. If you do not receive a confirmation from a company, you should contact that company directly to place a fraud alert.

Equifax: 1-800-525-6285; www.equifax.com; P.O. Box 740241, Atlanta, GA 30374-0241

Experian: 1-888-EXPERIAN (397-3742); www.experian.com; P.O. Box 9532, Allen, TX 75013

TransUnion: 1-800-680-7289; www.transunion.com; Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92834-6790

Once you place the fraud alert in your file, you're entitled to order one free copy of your credit report from each of the three consumer reporting companies, and, if you ask, only the last four digits of your Social Security number will appear on your credit reports. Once you get your credit reports, review them carefully. Look for inquiries from companies you haven't contacted, accounts you didn't open, and debts on your accounts that you can't explain. Check that information, like your Social Security number, address, name or initials, and employers are correct. If you find fraudulent or inaccurate information, get it removed. When you correct your credit report, use an Identity Theft Report with a cover letter explaining your request, to get the fastest and most complete results.

Continue to check your credit reports periodically, especially for the first year after you discover the identity theft to make sure no new fraudulent activity has occurred.

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 bureaus if your state is participating 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.

Step 3 File a report with the Federal Trade Commission and/or the Internet Crime Complaint Center.

You can go on-line to file an identity theft complaint with the FTC at www.consumer.gov/sentinel. Click on the "Identity Theft" icon. This website has very useful information if you are a victim of Identity Theft. You can also file a complaint by calling 1-877-IDTHEFT.

For **Internet** related crimes you can go online and file a complaint with the Internet Crime Complaint Center at www.ic3.gov.

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 can refer victims complaints to other government agencies and companies for further action, as well as investigate companies for violations of laws the agency enforces.

Additionally, you can provide a printed copy of your online Complaint form to the police to incorporate into their police report. The printed FTC ID Theft Complaint, in conjunction with the police report, can constitute an Identity Theft Report and entitle you to certain protections. This 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 report; (3) prevent a company from continuing to collect debts that result from identity theft; and (4) place an extended fraud alert on your credit report.

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, cell phone companies, etc. Provide the creditors with the completed Identity Theft Affidavit, Letter of Dispute, and a copy of the FACTA Law. Some companies may require that you use their own affidavit.

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 Rochester 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 subpoenas and/or court orders for the very same information. It allows you to request the information be made available to the Rochester 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 the Rochester Police Department.

To avoid confusion we request that you submit everything at once and if possible do not submit items separately. The types of document evidence needed for prosecution are on the next page. **Please remember 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 Rochester Police Department if you desire prosecution and are willing and available to appear and testify in court should a suspect be identified and arrested.**

You will be contacted by an investigator only if the document evidence you submit leads to the identification and prosecution of a suspect.

Additional Information

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/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 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 free PEBES application at your local Social Security office or at www.ssa.gov/online/ssa-7004.pdf .

Internal Revenue Service The IRS Office of Special Investigation can be contacted at www.irs.gov to report false tax filings, potential criminal violations of the Internal Revenue Code and related financial crimes.

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, Identity Theft Affidavit, Letter of Dispute and a copy of the FACTA Law.

Documentation for Prosecution

The following items of evidence should be obtained by the victim by using the sample dispute letters to dispute charges and requesting all documentation related to the account(s). Without this document evidence, we will not be able to begin an investigation.

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

- Bank statements or bills showing where the transactions occurred.
    - Please circle or underline the fraudulent transactions.
    - Using a highlighter may make it impossible to read photocopies.
    - Please attempt to obtain a physical address for the transactions from your bank.
- Bills from companies showing merchandise ordered.
    - Addresses where items were delivered.
    - What phone numbers were associated with the order.
- Any information from the creditor that shows how or where the account was used.
- The name or employee number and phone number of any representatives from the businesses you deal with.

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

- Bank statements that you may have received for accounts that are not yours.
- Credit reports showing the accounts that are not yours.
    - Please circle or underline the fraudulent transactions.
    - Using a highlighter may make it impossible to read photocopies.
- Bills from utility companies for accounts you did not open.
- Letters or documentation from creditors or utility companies that contain:
    - Copies of applications for credit.
    - How the account was opened. (In person, over the phone, on internet.)
    - Where the account was opened if done in person.
    - Where the account is being used (addresses of transactions.)
    - Addresses where any cards, bills, merchandise or correspondence was mailed.
    - Any phone numbers associated with the fraudulent account.
- The name or employee number and phone numbers of any representatives from the businesses you deal with.

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

- Copies of Department of Economic Security or Social Security Administration report showing your information being used for employment in Rochester.
- If 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.

Fair and Accurate Credit Transactions Act of 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 payments from, or otherwise entered into commercial transaction for consideration with, a person who has allegedly made unauthorized use of the means of identification of the victim, shall provide a coy 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 tie 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 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.

Identity Theft Affidavit

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 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

_____
(House Number) (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 (____) _____

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.
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, drivers 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, mothers

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 was used or how the identity thief gained access to your information)

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

(Attach additional pages as necessary)

Victim's Law Enforcement Actions

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 purpose 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 ☐ 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 Checklist

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 identification card, or your passport.) If you are under 16 and don't have a photo identification, 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 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.

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 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 imposition of a fine or imprisonment or both.

_____ _____
(Signature) (Date signed)

_____
(Notary)

(Check with each company as creditors sometimes require notarization. If they don't, please have one witness (non-relative) sign below that you completed and signed this affidavit.)

Witness:

_____ _____
(Signature) (Printed Name)

_____ _____
(Date) (Telephone Number)

Fraudulent Account Statement

Completing the Statement

- Make as may 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 goods/services)
Example Example National Bank 123 Main Street Columbus, OH 22722	01234567-89	Auto Loan	01/01/2008	$25,000.00

☐ 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
You're Name
You're 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 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 re-investigate this (these) matter(s) and (delete or correct) the 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 make these records available to the Rochester Police Department upon their request.** (It may be helpful to enclose a copy of the FACTA law with this letter).

Sincerely,

You're Name

Enclosures: (List what you are enclosing).

Sample Dispute Letter for Existing Accounts

Date
You're Name
You're Address
You're City, State, Zip Code
You're 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 re-instated), 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 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 make these records available to the Rochester Police Department upon their request.** (It may be helpful to enclose a copy of the FACTA law with this letter.)

Sincerely,

You're Name

Enclosures: (List what you are enclosing).

Taxpayer Guide to Identity Theft

Español 中文 한국어 TiếngViệt Русский

For 2017, the IRS, the states and the tax industry joined together to enact new safeguards and take additional actions to combat tax-related identity theft. Many of these safeguards will be invisible to you, but invaluable to our fight against these criminal syndicates. If you prepare your own return with tax software, you will see new log-on standards. Some states also have taken additional steps. See your state revenue agency's web site for additional details.

We also know identity theft is a frustrating process for victims. If you become a victim, we are committed to resolving your case as quickly as possible.

What is tax-related identity theft?

Tax-related identity theft occurs when someone uses your stolen Social Security number to file a tax return claiming a fraudulent refund.

You may be unaware that this has happened until you efile your return and discover that a return already has been filed using your SSN. Or, the IRS may send you a letter saying we have identified a suspicious return using your SSN.

Know the warning signs

Be alert to possible tax-related identity theft if you are contacted by the IRS or your tax professional/provider about:

- More than one tax return was filed using your SSN.
- You owe additional tax, 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 or other income from an employer for whom you did not work.

If you suspect you are a victim of identity theft, continue to pay your taxes and file your tax return, even if you must do so by paper.

Steps to take if you become a victim

If you are a victim of identity theft, the Federal Trade Commission recommends these steps:

- File a complaint with the FTC at identitytheft.gov.
- Contact one of the three major credit bureaus to place a 'fraud alert' on your credit records:
  - Equifax, www.Equifax.com, 1-888-766-0008
  - Experian, www.Experian.com, 1-888-397-3742
  - TransUnion, www.TransUnion.com, 1-800-680-7289
- Contact your financial institutions, and close any financial or credit accounts opened without your permission or tampered with by identity thieves.

If your SSN is compromised and you know or suspect you are a victim of tax-related identity theft, the IRS recommends these additional steps:

- Respond immediately to any IRS notice; call the number provided.
- Complete IRS Form 14039, Identity Theft Affidavit, if your efiled return rejects because of a duplicate filing under your SSN or you are instructed to do so. Use a fillable form at IRS.gov, print, then attach the form to your return and mail according to instructions.

If you previously contacted the IRS and did not have a resolution, contact us for specialized assistance at 1-800-908-4490. We have teams available to assist.

About data breaches and your taxes

Not all data breaches or computer hacks result in tax-related identity theft. It's important to know what type of personal information was stolen.

If you've been a victim of a data breach, keep in touch with the company to learn what it is doing to protect you and follow the "Steps for victims of identity theft." Data breach victims should submit a Form 14039, Identity Theft Affidavit, **only** if your Social Security number has been compromised and your efile return was rejected as a duplicate or IRS has informed you that you may be a victim of tax-related identity theft.

How to reduce your risk

Join efforts by the IRS, states and tax industry to protect your data. Taxes. Security. Together. We all have a role to play. Here's how you can help:

- Always use security software with firewall and anti-virus protections. Use strong passwords.
- Learn to recognize and avoid phishing emails, threatening calls and texts from thieves posing as legitimate organizations such as your bank, credit card companies and even the IRS.
- Do not click on links or download attachments from unknown or suspicious emails.
- Protect your personal data. Don't routinely carry your Social Security card, and make sure your tax records are secure.

See Publication 4524, Security Awareness for Taxpayers, to learn more**.**

The IRS does not initiate contact with taxpayers by email to request personal or financial information. This includes any type of electronic communication, such as text messages and social media channels.

Report suspicious online or emailed phishing scams to:phishing@irs.gov. For phishing scams by phone, fax or mail, call 1-800-366-4484. Report IRS impersonation scams to the Treasury Inspector General for Tax Administration's IRS Impersonation Scams Reporting.

See the main Identity Protection page for more information