# Protecting You and Your Clients from Fraud

Tax professionals continue to be a prime target of cybercriminals. We must all take responsibility for protecting client data from theft.

To provide you guidance on data security, the IRS joined with state agencies and the tax industry to form the Security Summit. The Security Summit has created awareness campaigns such as:

- Boost Security Immunity: Fight Against Identity Theft
- Protect Your Clients; Protect Yourself: Tax Security 101
- Tax Security 2.0
- Working Virtually: Protecting Tax Data at Home and at Work

This year's theme is "Protect Your Clients; Protect Yourself — Summer 2022" to urge tax professionals to watch out for vulnerabilities when using cloud-based services and to create a plan for data safety. As part of this campaign, the Security Summit partners recently released a document called Written Information Security Plan (WISP) designed to help tax professionals create and implement a data security plan.

### Secure Your Systems

Title V, Subtitle A of the Financial Services Modernization Act of 1999, also known as Gramm-Leach-Bliley Act, and the Safeguards Rule (16 CFR Part 314) require certain entities - including tax return preparers - to create and maintain a security plan for protecting client data.

According to the Federal Trade Commission (FTC), each company, as part of its plan, must:

- Designate one or more employees to coordinate its information security program.
- Identify and assess the risks to customer information in each relevant area of the company's operation and evaluate how effectively current safeguards control these risks.
- Design and implement a safeguards program with regular monitoring and testing.
- Select service providers who maintain appropriate safeguards. Ensure the contract requires the provider to maintain safeguards and oversee their handling of customer information.
- Evaluate and adjust the program in light of relevant circumstances, including changes in the firm's business or operations or results from security testing and monitoring.

Note that the FTC is re-evaluating the Safeguards Rule and has proposed new regulations. Watch for any changes in the Safeguards Rule and their effect on the tax preparation community.

These publications will help you get started:

- IRS Publication 4557 outlines your obligations to protect taxpayer information. It also has a checklist for creating and maintaining a security plan for your digital network and office.
- FTC Cybersecurity for Small Business includes practical tips for business on creating and implementing a plan for safeguarding personal information.

- NIST's Small Business Information Security – The Fundamentals (NISTIR 7621, Revision 1) provides small businesses an overview of five principles to secure data: identify, protect, detect, respond, and recover.
- IRS Publication 5293 provides basic steps you and your firm can take to protect client data. This step-by-step guide makes data security achievable for tax professionals and firms of all sizes.

## Spot Data Theft

You or your firm may be a victim of data theft and not even know it. Here are some common clues to data theft:

- Your clients' e-filed tax returns begin to be rejected because returns with their Social Security Numbers were already filed
- The number of returns filed for a taxable year with your firm's Electronic Filing Identification Number (EFIN) exceeds your number of clients
- Tax professionals or clients respond to emails you or your firm did not send
- Your network computers slow down
- Computer cursors move or numbers change without your input
- Network computers lock you out
- Your clients receive:
  - IRS authentication letters (Letters 5071C, 4883C, or 5747C) for returns they did not file
  - Refunds for returns they did not file
  - Tax transcripts they did not request
  - IRS online services account emails stating an account was created when they did not create one
  - IRS online services account emails stating their account was accessed or disabled when they did not request it

## Create a Data Theft Response Plan

If you fall victim to data theft, immediately:

- **Report it to the** local IRS stakeholder liaison. Stakeholder liaisons will notify IRS Criminal Investigation and others within the agency. The IRS can block fraudulent returns in the clients' names and assist through the process. If the data theft involved an IRS impersonation scam, you should also report it to the Treasury Inspector General for Tax Administration.
- **Email the Federation of Tax Administrators at** StateAlert@taxadmin.org**.** Get information on how to report victim information to the states. Most states require that the state attorney general be notified of data breaches. The notification process may involve multiple offices.
- **Call the Minnesota Department of Revenue** at 651-296-3781 or 1-800-652-9094. We will connect you with a fraud coordinator who can assist with determining whether you are a victim and which clients' or tax professionals' information was accessed. We can take steps to block fraudulent returns in your clients' names.

- **Submit an identity theft affidavit for businesses and other entities**. Federal Form 14039-B makes it easier for businesses, estates, trusts, and tax-exempt organizations to report identity theft to the IRS. Submitting this form will quickly let the IRS help entities who are victims of identity theft. To access the form, see Report Identify Theft for a Business on the IRS website.

Find Data Theft Information for Tax Professionals on the IRS website.

## Stay Vigilant

Stay ahead of the thieves by taking certain actions daily or weekly to ensure your clients and your business remain safe:

- **Track your daily e-file acknowledgements.** If there are more acknowledgements than returns you know you filed, dig deeper.
- **Track your weekly Electronic Filing Identification Number (EFIN) usage.** The IRS posts the number of returns filed with your EFIN weekly.
    - Access your IRS e-Services account and your EFIN application
    - Select "EFIN Status" from the application
    - Contact the IRS e-help Desk if your return totals exceed your number of returns filed
    - Keep your EFIN application up to date with all phone, address, or personnel changes
- **Track your weekly Preparer Tax Identification Number (PTIN) usage.** If you file 50 or more returns as an attorney, Certified Public Accountant (CPA), enrolled agent (EA), or Annual Filing Season Program participant, you can check your PTIN account for a weekly report.
    - Access your online PTIN account
    - Select "View Returns Filed Per PTIN"
    - Complete federal Form 14157 to report excessive use or misuse of your PTIN
- **If you have a Centralized Authorization File (CAF) Number,** keep your authorizations up to date. Use a Freedom of Information Act (FOIA) request to secure your CAF 77 client listing. Review the list to ensure it is accurate. Remove authorizations for clients you no longer work with and for any taxpayers who have never been your clients (a possible ID theft indicator). For more information, see IRS Publication 947.
- **Create your IRS online accounts using the multi-factor Secure Access authentication** to help prevent account takeovers. For details, see the IRS's Secure Access page.

## Recognize Phishing Scams

Cybercriminals commonly steal data through phishing scams. Phishing often occurs through unsolicited emails or websites luring unsuspecting victims to provide personal information.

The thief may pose as your tax software provider, your data storage provider, your bank, the IRS, or even a prospective client. Thieves may even pose as colleagues whose email accounts were compromised. For tips on defending yourself from phishing scams, see Report Phishing and Online Scams from the IRS.

Educate all employees in your office on the dangers of phishing scams. These scams can result in cybercriminals taking over your computer or accounts to steal client data.

- Thieves may hijack your email account to send spam emails under your name, tricking your colleagues and clients into disclosing information
- An even more successful tactic is spear-phishing, where a thief specifically targets you or your firm, perhaps from seeing your email address online
- Generally, phishing or spear-phishing emails have an urgent subject line such as "Update Your Account Now," enticing you to open a link or attachment
    - **Link:** The link may take you to a fake webpage designed to look like a familiar website such as IRS e-Services. There may also be a call to action, such as "Click Here Now." You may be asked to enter your username and password for an account, but you are actually disclosing your credentials to thieves.
    - **Attachment:** Attachments may contain software that can infect your computer and network systems (malware). A common malware is keystroke tracking, which allows the criminal to see the words you type on your device, including your username and password to various accounts. This malware gives them access to your tax software, bank, or encrypted client files.
- A legitimate business should never request personal or sensitive information be sent to them via email, unless through a secured mail service

## Guard Against Phishing Emails

Educated employees are the key to avoiding phishing scams, but these simple steps can also help protect you:

- Use separate personal and business email accounts protected with strong passwords and multi-factor authentication
- Install an anti-phishing toolbar, which may be included in security software products, to help identify known phishing sites
- Use security software to help protect systems from malware and scan emails for viruses
- Never open or download attachments from unknown senders, including potential clients; try calling them first
- If you must email files with clients, send only encrypted and password-protected documents
- Do not respond to suspicious or unknown emails; if suspicious emails are IRS-related, forward them to phishing@irs.gov

## Be Safe on the Internet

Data security takes an ongoing awareness about the threats posed from a variety of sources, including browsing the internet. Here are some general steps for staying safe online.

- Keep your web browser software up to date so it has the latest security features
- Scan files using your security software before downloading them
- Delete web browser cache, temporary internet files, cookies, and browsing history regularly

- When possible, only use web addresses that start with "HTTPS" (https://www.irs.gov)
- Avoid accessing business emails or information from public Wi-Fi connections
- Disable stored password features offered by some operating systems
- Enable your browser's pop-up blocker and do not call numbers from pop-ups
- Do not download files, software, or applications from unknown websites
- Note instances where your browser's home page changes; this could be a sign of malware or intrusion
- Use a Virtual Private Network (VPN) - a secure, encrypted tunnel to transmit data between a remote user and the company network

## Stay Connected

We alert tax professionals as quickly as possible when we learn of new scams, which are especially common during the filing season. Sign up for our email updates so you can stay informed of the latest alerts and tax administration issues:

1. Go to www.revenue.state.mn.us and select the gray envelope on the bottom right
2. Enter your email address
3. Check the "Tax Scam and Fraud Alerts" box under Tax Professionals
4. Select Submit

## Encourage clients to obtain Identity Protection PINs (IP PINs)

The IP PIN Opt-In Program can protect taxpayers against tax-related identity theft and is available to anyone who can verify their identity. The program is a free way for taxpayers to protect themselves, but we need your help to inform them of it. For details, see Get An Identity Protection PIN on the IRS website or see IRS Publication 5367.

For security reasons, you cannot obtain an IP PIN on behalf of clients. They must obtain their own IP PIN.

## New State Forms to Help Report ID Theft

In an effort to better support identity theft victims, we released new forms in 2021. These forms help manage the reporting of identity theft to Revenue and allow your clients to request copies of fraudulently filed returns.

If your client believes they are a victim of identity theft, they should call us at 651-296-3781 or 1-800-652-9094. Then, they should complete and submit Form M1ID, Identity Theft Affidavit. This will alert us of the issue and help in detection of any potential fraud on their account. We will notify your client if a fraudulent return was filed or not.

If your client receives a letter informing them a Minnesota return was fraudulently filed under their name, they can contact us for a copy of the return.

- If your client wants a copy of the fraudulent return for their records, they should complete Form REV189, Request for Copy of Return Related to Identity Theft

- If your client wants to send a copy of the fraudulent return to a specific law enforcement agency, they should complete Form REV190, Authorization to Release Return Related to Identity Theft

For reference, we have included samples of these forms on the following pages.

DEPARTMENT OF REVENUE

# Form M1ID, Identity Theft Affidavit

This form allows you to inform the Minnesota Department of Revenue that your tax return may be impacted by identity theft.

## Section A — Name and Contact Information of Taxpayer

Taxpayer Name

Social Security Number or ITIN

Street Address or PO Box

Apartment or Suite

Minnesota or Federal Employer Identification Number (FEIN) (Sole Proprietors)

City

State

ZIP Code

Primary Language

Phone Number

Email Address (Optional)

**Attach the following documentation to Form M1ID:**

- A copy of one document to verify your identity, such as a driver's license, U.S. passport, US Military ID card, or other valid ID issued by state or federal government.
- A copy of one or more documents showing your address for the affected tax years, such as a utility bill, lease agreement, or bank statement. If not applicable, provide proof of your current address.
- A copy of all wage and tax statements issued to you during the affected tax years.
- A copy, if any, of a police report regarding the identity theft.

## Section B — Identity Theft Victim Details

Check the following boxes in this section that apply to the specific situation you are reporting:

☐ I am submitting this form for myself.

☐ I am submitting this form in response to a Letter received from the Minnesota Department of Revenue.
Please provide any relevant Letter ID numbers.

☐ I am submitting this form on behalf of my dependent child or dependent relative.

☐ I am submitting this form as the appointed conservator or due to being awarded power of attorney.

☐ I am submitting this form on behalf of a deceased taxpayer. (If yes, include a copy of the death certificate.)

## Section C — Reason for Filing this Form

☐ Someone used my information to file taxes

☐ I do not know if someone used my information to file taxes, but I am a victim of identity theft.

## Section D — Identity Theft Details

How did you learn of the identity theft? (Explain your identity theft issue, how you became aware of it, and provide relevant dates.)

What tax years are you claiming your identity was stolen?

Were you a Minnesota resident during the years your identity was stolen? ☐ Yes ☐ No

Were you required to file a Minnesota individual income tax return? ☐ Yes ☐ No

Were you incarcerated during the tax years in question? ☐ Yes ☐ No

Date of incarceration: to

Location of incarceration (name of location, city, state):

*Continued*

## Form M1ID, Identity Theft Affidavit, page 2

**Section E — Employer or Preparer Data Breach**

Was your identity compromised because of an employer or preparer data breach? ☐ Yes ☐ No

If yes, include a copy of the notification letter or an email provided by your employer or preparer.

What is the name of your employer or preparer?

What is the best contact number for your employer or preparer?

If known, when and how did the data breach occur?

**Section F — Additional Steps Recommended After Submission**

1. Contact the Internal Revenue Service (IRS). Include a copy of the Federal Form 14039 (Identity Theft Affidavit), if required by the IRS. Visit www.identitytheft.gov for more information.
2. File a police report with your local police department. Obtain a copy of the police report for your own records
3. Contact the following governmental entities to notify them that your identity was stolen:
   a. Federal Trade Commission: www.ftc.gov or call 1-877-438-4338
   b. Social Security Administration: www.socialsecurity.gov or call 1-800-772-1213
4. Contact the following credit bureaus to notify them that your identity was stolen:
   a. Equifax: www.equifax.com or call 1-800-525-6285
   b. Experian: www.experian.com or call 1-888-397-3742
   c. TransUnion: www.transunion.com or call 1-800-680-7289

**Section G — Penalty of Perjury Statement and Signature**

**I hereby state that the above information on this Form M1ID is true and correct, and that all relevant information has been included.**

*Parent, Guardian, Conservator: I certify that I have the legal authority to sign this form.*

| Signature | Date | Address, if Different from Taxpayer | | |
|---|---|---|---|---|
| | / / | | | |
| **Print Name and Title** | **Phone Number** | **City** | **State** | **ZIP Code** |
| | | | | |

**Mail:** Minnesota Department of Revenue, PO Box 64598, St. Paul, MN 55164-0598
**Fax:** 651-556-5144 (Attn: ID Theft)

# Form M1ID Instructions

## Purpose of This Form

By signing Form M1ID, you authorize the Minnesota Department of Revenue to indicate that your tax returns may be impacted by identity theft.

## How to Complete this Form

The way you complete this form depends on whether you have a Minnesota Individual Income Tax filing requirement. To determine if you have a filing requirement, go to www.revenue.state.mn.us and enter **who must file** into the Search box.

Allow us at least 60 days to review your response upon receipt. If you fail to provide all the required documents in this affidavit, your claim may be delayed or deemed unsubstantiated.

## Victims with a filing requirement

File a paper Minnesota Income Tax return (Form M1, *Individual Income Tax*) and mail to the appropriate address listed on the return. Attach to your return all income source documents (such as employer-issued W-2s and 1099s) and any applicable schedules.

Once you have your return, complete Form M1ID and mail or fax it to the address or fax number listed on the form. Include your return (with all attachments) and a completed copy of federal Form 14039. You may also attach a police report you filed for the identity theft.

Keep copies of your return and documents for your records.

## Victims without a filing requirement

Mail or fax a fully completed Form M1ID, to the address or fax number listed on the form. You may also attach a police report you filed for the identity theft. Keep copies of all documents for your records.

## Your Signature

This affidavit is not valid unless it is signed and dated by someone with legal authority to sign it. For most people, this is the taxpayer whose data is being shared.

If granting authority for a joint return, only one spouse needs to sign. Parents or legal guardians must sign for minors. For legal guardians, conservators, personal representatives, and others signing on the taxpayer's behalf, we require documents and a photo ID to confirm legal authority.

We may request additional information as needed.

## Questions?

For details about how identity theft and how the Minnesota Department of Revenue protect you from it, visit our website and enter **identity theft** into the Search box.

You may also contact us.

Income Tax and Withholding Division
Phone: 651-297-5195 or 1-800-657-3500
Email: individual.incometax@state.mn.us

This information is available in alternative formats.

DEPARTMENT OF REVENUE

# Form REV189, Request for Copy of Return Related to Identity Theft

To authorize the department to the release a copy of a return related to identity theft to a designated recipient at a law enforcement agency use Form REV190, *Authorization to Release Return Related to Identity Theft*.

**Taxpayer/Victim**

| Taxpayer Name | | | Social Security Number or ITIN | |
|---|---|---|---|---|
| Street Address or PO Box | Apt. or Suite | | Phone Number | Fax Number |
| City | State | ZIP Code | Email Address *(Optional)* | |

**Type of Tax Return**

| Type of Tax Return You are Requesting | Tax Form Name or Number | Tax Year or Period |
|---|---|---|
| | | |
| | | |
| | | |

**Signature**

**This form is not valid until signed and dated by the taxpayer.**

*Parent, Guardian, Conservator: I certify that I have the legal authority to sign this form.*

| Signature | Date | Address, If Different from Taxpayer | | |
|---|---|---|---|---|
| | / / | | | |
| Print Name and Title, If Applicable | Phone Number | City | State | ZIP Code |
| | | | | |

Send a signed copy of this form to the department:

Mail: Minnesota Department of Revenue
P.O. Box 64598
St. Paul, MN 55164-0598

Fax: 651-556-5144 (Attn: ID Theft)

## Form REV189 Instructions

### Purpose of This Form

By signing this form, you request that the Minnesota Department of Revenue provide you a copy of one or more tax returns listed above that used your name and/or Social Security number filed by a third-party without your consent (identity theft) with the department. For any such return, this is your private data.

### Your Signature

This authorization is not valid until it is signed and dated by someone with legal authority to sign it. For most people, this is the taxpayer whose data is being shared.

If granting authority for a joint return, only one spouse needs to sign. Parents or legal guardians must sign for minors. For legal guardians, conservators, personal representatives, and others signing on behalf of the taxpayer, we require documents and a photo ID to confirm your legal authority.

We reserve the right to request additional information as needed.

### Questions?

Website: www.revenue.state.mn.us
Phone: 651-297-5195 or 800-657-3500

DEPARTMENT OF REVENUE

# Form REV190, Authorization to Release Return Related to Identity Theft

To authorize the department to the release a copy of a return related to identity theft for yourself use Form REV189, *Request for Copy of Return Related to Identity Theft.*

**Taxpayer/Victim**

| Taxpayer Name | | | Social Security Number or ITIN |
|---|---|---|---|
| Street Address or PO Box | | | Minnesota or Federal Employer Identification Number (FEIN)(Sole Proprietors) |
| Apt. or Suite | | | Phone Number / Fax Number |
| City | State | ZIP Code | Email Address |

**Type of Tax Return**

| Type of Tax Return You are Requesting | Tax Form Name or Number | Tax Year or Period |
|---|---|---|
| | | |
| | | |
| | | |

**Recipient**

I authorize the Minnesota Department of Revenue to disclose to the designated recipient at the law enforcement agency listed below to receive information related to the tax return(s) listed above.

| Name of Law Enforcement Agency | | | Recipient Official's Name and Title |
|---|---|---|---|
| Street Address or PO Box | | | Phone Number |
| Suite | | | Fax Number |
| City | State | ZIP Code | Email Address |

**Signature**

I understand that this includes information related to the purported return that was filed by a third party using my name and/or Social Security Number without my knowledge or consent, for the tax year or period listed above. This information includes a copy of the return, any attachments to the return, and transmission data tied to the return (if filed electronically). This information would not include the identity of, or any investigatory information regarding, the third party who filed the purported return.

I also understand that the law enforcement agency designated above may use this information to investigate and/or prosecute any person(s) who may have been involved in the filing of the purported return or other crimes related to the use of my identifying information. In addition, I further understand that the law enforcement agency designated above may share this information with other law enforcement agencies directly involved in this or other investigations and/or prosecutions of crimes related to the use of my identifying information by these persons.

**Do not sign this form if it is blank or incomplete.** ***I certify that I am the taxpayer whose name and/or Social Security number was used to file my purported return.*** *Parent, Guardian, Conservator: I certify that I have the legal authority to sign this form.*

| Signature | Date | Address, If Different from Taxpayer | | |
|---|---|---|---|---|
| | / / | | | |
| **Print Name and Title** | **Phone Number** | **City** | **State** | **ZIP Code** |
| | | | | |

Send a signed copy of this form to the department:
Mail: Minnesota Department of Revenue, Mail Station 6590, 600 Robert Street North, St. Paul, MN 55146
Fax: 651-556-5210

## Form REV190 Instructions

### Purpose of This Form

By signing this form, you authorize the Minnesota Department of Revenue to release your private data from one or more tax returns listed above related to identity theft to the designated recipient at the law enforcement agency named above.

The designated recipient above may inspect and receive your private data but may not act on your behalf.

### Your Signature

This authorization is not valid until it is signed and dated by someone with legal authority to sign it. For most people, this is the taxpayer whose data is being shared.

If granting authority for a joint return, only one spouse needs to sign. Parents or legal guardians must sign for minors. For legal guardians, conservators, personal representatives, and others signing on behalf of the taxpayer, we require documents and a photo ID to confirm your legal authority.

We reserve the right to request additional information as needed.

### Expiration

This authorization expires once the data is released.

### Questions?

Website: www.revenue.state.mn.us
Phone: 651-297-5195 or 800-657-3500