

Minnesota Leads Reporting Requirements

The Minnesota Department of Revenue established leads reporting requirements for all software providers transmitting Individual Income tax or Property Tax Refund returns to help fight identity theft and fraud.

Data Submission Requirements

What will software providers report to Minnesota Department of Revenue?

You must submit a report using our defined schema that aligns with patterns defined below or other suspicious activity observed in your products. You should include the report code(s) that most closely identify the type of activity observed. Minnesota uses the report code(s) in combination with additional fraud filters to sort returns for review. By providing the report code you help us to reduce false positives and review returns most efficiently.

Please Note: The patterns below are minimum standards. If you identify other suspicious or potentially fraudulent behavior, we expect you to share that information with us by contacting us at 651-556-4818 or e-mail us at Efile.DevSupport@state.mn.us.

Minimum Standards - DIY

Report Code	Pattern Identifier	Pattern Description
01	Improper Account Access	After the point of return filing: <ol style="list-style-type: none"> 1. A customer notifies the vendor that their account was accessed improperly, or 2. A vendor identifies an account takeover or account access resulting from stolen credentials occurred.
02	Password Resets	A customer is required to reset their password AND they successfully accessed their account less than 30 days prior to password reset. <i>Example:</i> A returning customer successfully logs in to their account on February 1 to begin preparing return, then attempts to log in again on February 15 and fails to the point that they must reset their password.
03	Suspicious Login Duration	Return associated with a device that logs into any single session for < 1 minute.

Report Code	Pattern Identifier	Pattern Description
04	Email Addresses- Random Keystroke Emails	SSNs that file a refund request using random keystroke email addresses. For example: fdjadjkfkaldkjfdkfdkjfdkjeieurekj@gmail.com. Some examples, but not limited to: <ol style="list-style-type: none"> 1. All letters on the same row of keyboard 2. All the same character 3. Repeating pattern of characters alternating back and forth (asdfasdf, afafafafaf)
05	More than X IPAs	One return accessed by more than X* IPAs.
06	More than X DeviceIDs	One return accessed by more than X* Device IDs.
07	Multiple returns from one account with no Preparer ID	A single user ID submits more than 20 returns with no Preparer ID and no FEIN.
08	High Risk IP Address	More than X* distinct state returns that are submitted from atypical IP Address where 'atypical' is defined by the software provider based on their own analysis of fraud in their product(s).
09	High Risk UBA	More than X* distinct state returns that file a refund request using the same UBA.
10	High Risk Physical Address	More than X* distinct state returns that file a refund request using the same Physical Address.
11	High Risk Phone Number	More than X* distinct state returns that file a refund request using the same Phone Number.
12	Other	The lead is being submitted for a reason that is not defined above. Additional information should be provided using Elements 23 and/or 24.

Where X is defined by the software provider based on their own analysis of fraud in their product(s). X may vary for each platform, product, and/or provider. You may define X differently for IP Addresses than for UBA, etc. Provide department your X values by email to Efile.DevSupport@state.mn.us.

Minimum Standards - Professional

Report Code	Pattern Identifier	Pattern Description
01	Improper Account Access	After the point of return filing: 3. A customer notifies the vendor that their account was accessed improperly, or 4. A vendor identifies an account takeover or account access resulting from stolen credentials occurred.
02	Not required for Pro	Not required for Pro.
03	Not required for Pro	Not required for Pro.
04	Not required for Pro	Not required for Pro.
05	More than X IPAs	One return accessed by more than X* IPAs.
06	More than X DeviceIDs	One return accessed by more than X* Device IDs.
07	Not required for Pro	Not required for Pro.
08	High Risk IP Address	More than X* distinct state returns that are submitted from atypical IP Address where 'atypical' is defined by the software provider based on their own analysis of fraud in their product(s).
09	High Risk UBA	More than X* distinct state returns that file a refund request using the same UBA.

Report Code	Pattern Identifier	Pattern Description
10	High Risk Physical Address	More than X* distinct state returns that file a refund request using the same Physical Address.
11	High Risk Phone Number	More than X* distinct state returns that file a refund request using the same Phone Number.
12	Other	The lead is being submitted for a reason that is not defined above. Additional information should be provided using Elements 23 and/or 24.

Where X is defined by the software provider based on their own analysis of fraud in their product(s). X may vary for each platform, product, and/or provider. You may define X differently for IP Addresses than for UBA, etc. Provide department your X values by email to Efile.DevSupport@state.mn.us.

How will providers send information to Minnesota Revenue?

Minnesota uses MOVEit DMZ as a secure FTP solution for certified providers to send the state specific fraud leads reporting to Minnesota as well as retrieve the feedback report from Minnesota. This solution will have two options for connecting:

1. A secure web interface that requires a username and password to gain access to manually upload and download files.
2. Secure FTP client using SSH; username, password, and a certificate will be used to authenticate and secure the file transmissions.

How do I get a username and password for the FTP system?

You must provide the following information for creation of a username and password or association to a certificate:

- Name
- Phone number
- Email address
- IP address of the system connecting to the Secure FTP solution

An email will be sent containing the username, temporary password, and procedures for how to connect to Minnesota's Secure FTP solution.

What are the requirements of a lead reporting file sent to Minnesota?

Data File Type	File Name
XML	#####_MDORLEADRPT_***_??_YYYYMMDD.xml

File Name Legend

- ##### = Vendor Code (assigned user/folder name)
- MDORLEADRPT = Minnesota Department of Revenue Lead Reports
- *** = Testing or Production file (TST = Testing; PRD = Production)
- ??? = Sequence number (this is if more than one file is sent in a day or a resubmission is needed)
- YYYYMMDD = Year/Month/Day

Providers must have a process for resending/reposting the State Lead file should problems occur.

What are the requirements of a feedback report sent from Minnesota?

Data File Type	File Name
Compressed XML (zipped)	#####_MDORLEADFDBK_***_??_YYYYMMDD.zip

File Name Legend

- ##### = Vendor Code (assigned user/folder name)
- MDORLEADFDBK = Minnesota Department of Revenue Lead Feedback Report
- *** = Testing or Production file (MNS = Testing; MNP = Production)
- ??? = Sequence number (this is if more than one file is sent in a day or a resubmission is needed)
- YYYYMMDD = Year/Month/Day

Providers can contact the Minnesota DevSupport team at Efile.DevSupport@state.mn.us should a lead feedback report need to be resent/reposted.

When should software providers send Minnesota fraud leads reporting information?

You should submit fraud lead reports within 8 days of the return submission. If possible fraud activity is detected, send lead reports sooner. The reporting service is available 24 hours a day, 7 days a week.

If you identify an urgent issue, lead reporting information should be sent immediately and you should follow-up with an email to Efile.DevSupport@state.mn.us or call 651-556-4818.

If you have not identified any suspicious activity, you don't need to send us a report for that week. **However**, if we identify fraudulent returns and you have not submitted lead reports, we will contact you and if necessary, take additional action.

What will Minnesota Revenue report to providers?

The report includes information about your submissions at the provider level. It will include a summary of DIY and professional product together. We will deposit the XML file and you will receive an email notification when the report is available for you. Information included in the report is included in our schema.

How is Minnesota Revenue sharing with the National Fraud Summit?

We will share information about which data elements are useful in detecting fraud and new discoveries from the information submitted to Minnesota.

Each software provider, state, and the IRS are unique and fraud patterns and schemes can vary, we believe there is value in sharing Minnesota's experience with the Fraud Summit team.

Sharing in this way will help keep us ahead of schedule and identify additional ways to fight against fraud.

Minnesota Leads Reporting Testing Requirements

Each product transmitting Individual Income tax and/or Property Tax Refund returns must pass leads reporting testing before it will be allowed to transmit returns to the Minnesota Department of Revenue.

How will providers send leads reporting test cases to Minnesota Revenue?

Software providers must submit one Lead Report. The test case must:

- Include a Lead identifying each product and their ApplicationType, if applicable.
- Each field completed with fictitious information.
- Submit through MOVEit Cert.

Leads reporting testing opens on November 15, 2017.