



# Identity Theft & Taxes: How to Untangle Your Worst Nightmare

By Pat Hammond, The Business Guild

*There is no way to sugarcoat it. Reports of identity theft doubled in 2020 and this year's numbers are on track to be even higher.*

According to the Federal Trade Commission (FTC), there were 1,387,597 reports of identity theft in 2020, with 406,560 victims stating their identity was used to apply for a government document or benefit. In 2019, those numbers were 650,523 and 23,236, respectively.

While this is worrisome for anyone, it's even more problematic for sole proprietors, partners, and limited liability companies who file business income and losses with their personal taxes.

This is worse than lost returns or missing refunds.

Identity theft can destroy your ability to qualify for loans, lines of credit, or even government contracts. Imagine someone using your identity to take out loans, apply for unemployment, or commit a crime.

Once you let that idea sink in, consider the complication of someone stealing your employer identification number (EIN).

Small business owners are twice as vulnerable as the average citizen and there is little they can do to prevent it.

You can follow **best practices** for data security, but there have been so many high-profile data breaches, including a few incursions into IRS databases, that you have to assume your identity is already on the dark web.

With this in mind, let's look at how the IRS handles identity theft for you and your business.

For many people, the first sign someone has stolen their identity is when they try to file their taxes. If someone has already used your credentials to file a tax return, one of two things is going to happen.

1. The IRS will reject your tax return
2. You will receive **Letter 4883C** from the IRS Tax Payer Protection Program about suspicious activity with your identity

The IRS knows that identity theft is on the rise and has a system in place for helping taxpayers untangle their tax fraud nightmare, but it is the IRS. The process will require a fair amount of

# Identity theft losses rose to \$43 million in 2020

documentation and may take months, if not longer.

## **Scenario #1: The IRS Rejects Your Tax Return**

If your tax return is rejected, the IRS advises taxpayers to file a paper tax return with Form 14039, Identity Theft Affidavit completed and attached to the back. Once the IRS has received these items, they will assign your case to the Identity Theft Victim Assistance unit (IDTVA).

Per the IRS website, IDTVA will try to determine if this is the first instance or if your identity was used for other tax years. They will also need to investigate how many other people are

affected by the fraudulent return and verify all the names and associated social numbers (SSN) listed on both the real and fraudulent returns.

The IRS says it usually takes about 120 days but warns that the time to resolution has increased to 260 days because of the pandemic. Considering the explosion of identity theft cases since 2020, it would be safe to assume those times will be extended for 2021's taxes.

## **The IRS requests you do not contact them for status updates after submitting Form 14039.**

They will contact you if they need further information and you will receive

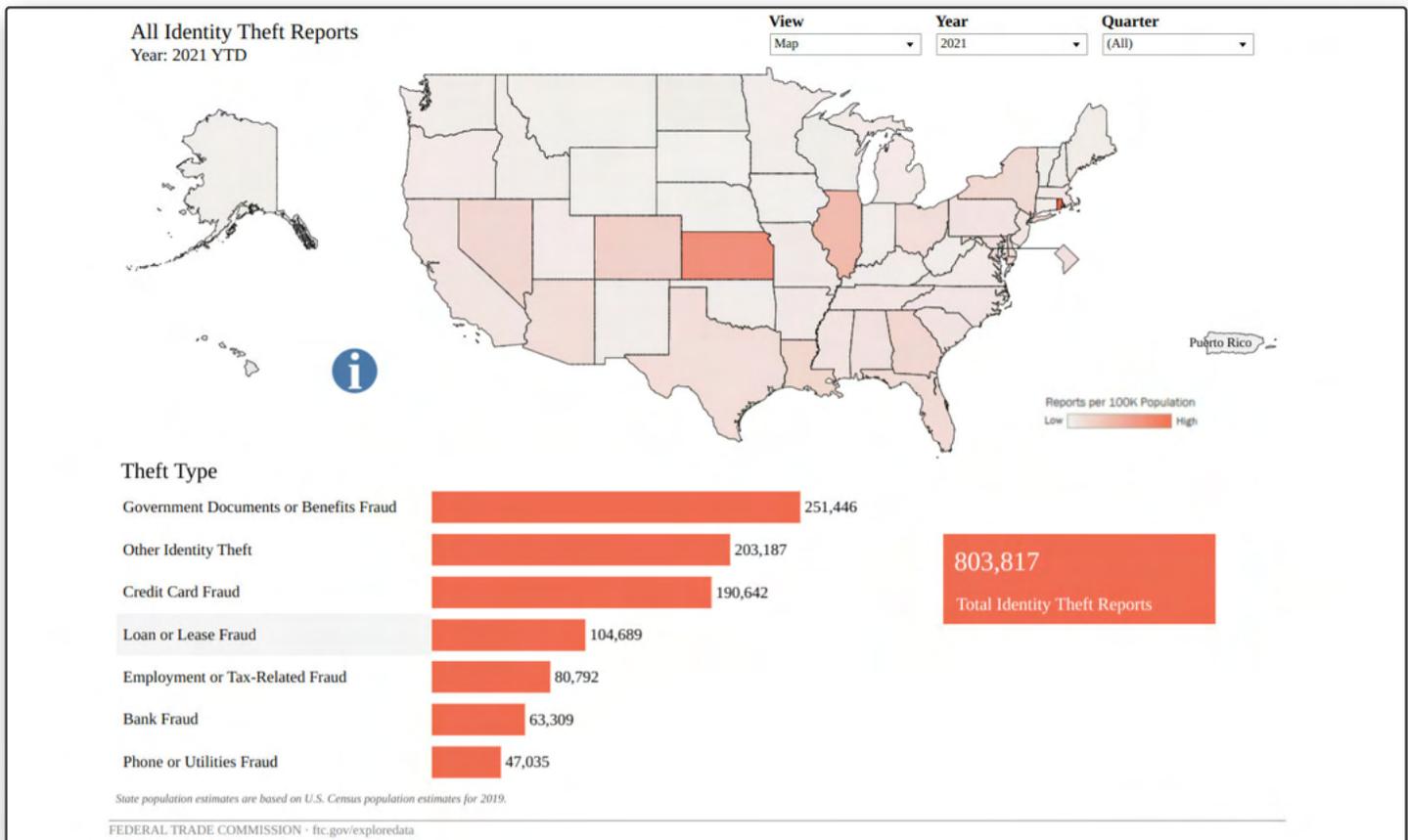
notification once your case is resolved.

They also state "Certain tax-related identity theft victims will be placed into the Identity Protection PIN program and annually receive a new, six-digit IP PIN." They do not, however, provide any information about how a person qualifies for this extra layer of protection.

## **Scenario #2: The IRS Notifies You of Suspicious Activity**

Your journey will be slightly different if the IRS notifies you about suspicious activity. The IRS will require that you prove you are who you say you are before discussing your case. You have 30 days to respond to their identification verification request, otherwise known as Letter 4883C, from the Taxpayer Protection Program.

They advise you to "follow the letter's instructions" when verifying your identity and to have the



letter with you when you call the toll-free number provided in the letter. You should also have a copy of your previous year's return. If you cannot convince the customer service representative of your identity, you may have to make an in-person visit to an **IRS Taxpayer Assistance Center**. This will require a photo ID along with Letter 4883C and a copy of the prior year's tax return. Once you prove your identity, the IRS will ask if

you filed the return in question. If you didn't, they will remove it from your tax records. If you confirm you filed the return, they will release it to be processed as normal.

The IRS offers no guidelines for how long this process takes but suggests you file a paper return if you have not yet filed for the current filing season.

### **Business Identity Theft**

Although business identity theft is much less common than individual identity

theft, it is still troublesome. A January 2020 report from the General Accountability Office (GAO) stated the IRS flagged 182,700 business tax returns for potential identity theft between January 2017 and August 2019. Only 4% of the returns, representing \$384 million in refunds, were "confirmed as business identity theft," but it's still a concern.

Given the drastic increase of reports of personal identity theft since 2019

## Compare Identity Theft Report Types

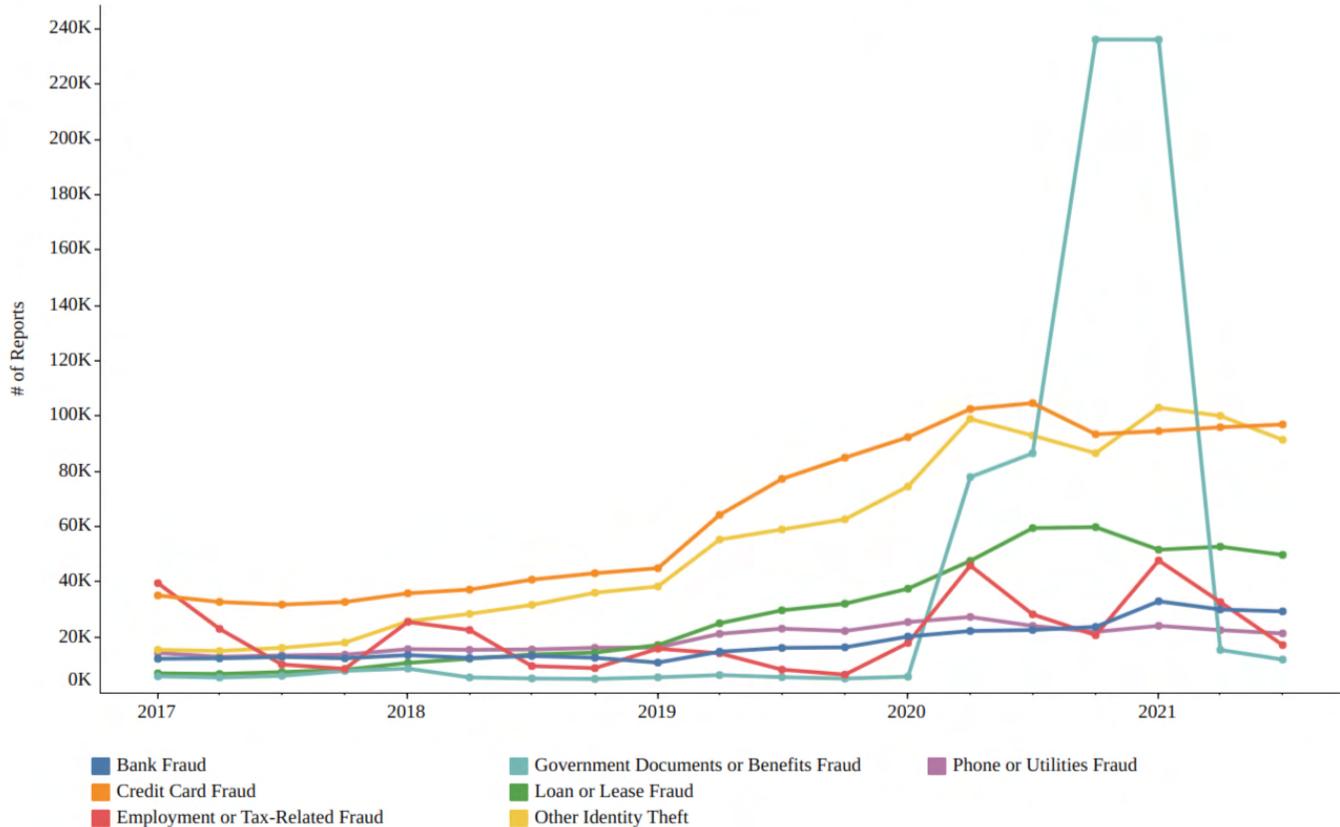
Date Range

2017 Q1

2021 Q3

Theft Type

(All)



Consumers can report multiple types of identity theft.

FEDERAL TRADE COMMISSION · [ftc.gov/exploredata](https://ftc.gov/exploredata)

and the number of pandemic-related assistance programs for American businesses, it is not a stretch to assume those numbers have also escalated over the past year and a half.

There are few resources available for business owners who suspect someone stole their business identity.

Unlike personal identity

theft, the FTC does not appear to provide a reporting mechanism for business owners who are victims of business identity theft. Other than a general suggestion to report the theft to your local police or the FBI, the U.S.

government doesn't offer much guidance on how to make an official complaint.

The only exception to this is tax fraud.

There may not be an official statistic for how many businesses are victims or how many returns the IRS determines are fraudulent, but the IRS has a procedure for you to follow if you suspect your EIN has been used to file a fraudulent tax return.

Unless you received an information request letter from them, the IRS asks business owners to submit

# It takes an average of six months & 200 hours to recover your identity

Form 14039-B, Business Identity Theft Affidavit to report suspected tax fraud because of business identity theft.

Like personal identity theft, you'll know your EIN has been used to file a fraudulent tax form if:

- The IRS rejects your e-filed return because someone else already filed a return with your EIN
- You receive a rejection to an extension request because someone already filed a return
- You don't receive routine notices from the IRS because someone else has

changed your business address

- You receive a letter or notice about something you didn't submit

You don't need to submit Form 14039-B if you receive a Letter 6042C or 5263C information request to validate a return or business entity. All you need to do is follow the instructions in the letter and respond within the designated time frame.

This is an area where a professional tax advisor can be invaluable. The IRS sends routine advisory notices to certified public accountants about new procedures and emerging

tax issues. Your CPA can help you identify fraudulent activity and help you navigate the IRS's sometimes Byzantine processes.

If you believe you or your business is a victim of tax identity theft, assume your company's banking and credit accounts are also at risk.

Follow standard precautions such as placing freezes or holds on credit and bank accounts, updating passwords, and monitoring your accounts.

Once the bad guys have your EIN or SSN it's easy for them to take the next step to take out loans or drain your bank accounts. ✓

[identitytheft.gov](https://identitytheft.gov)