

# Tax-Related Identity Theft

## HOW TO BETTER DETECT AND AVOID IT



Did you know that individual tax refunds are a prime target for cybercriminals looking to cash in on stolen identities?<sup>1</sup> According to the IRS, there were 597,000 tax returns with confirmed cases of identity theft in 2017 and 883,000 cases in the year prior.<sup>2</sup>

It's called **tax-related identity theft**, and it occurs when **a criminal uses a stolen Social Security number to claim a tax refund in the victim's name.**<sup>3</sup> The unfortunate victim may then have to spend months rectifying false deductions, incorrectly reported income, and other lingering issues with their tax return.<sup>4</sup>

Although the Internal Revenue Service (IRS) has attempted to combat tax identity theft in recent years, the responsibility to protect your personal information begins with you — the taxpayer.<sup>1</sup> That's why this paper is meant to educate you on how tax-related identity theft can occur and how to recognize the warning signs as well as common tactics used by scammers. We'll also cover preventative steps you can take to help better protect yourself and your loved ones from tax-related identity theft.

## What Is Tax-Related Identity Theft?

According to the IRS, **tax-related identity theft is one of the most common tax scams**, and it's most prevalent during filing season when taxpayers are preparing their returns on their own or hiring a tax professional to assist them.<sup>5</sup>

Identity thieves can get a victim's Social Security number in a variety of ways, such as through a data breach, stolen mail or W-2s, an impersonation scam, an unscrupulous tax preparer, or even an unsecured public Wi-Fi network. With stolen information in hand, the thief can then file a fraudulent tax return and enter their own payment details.<sup>6</sup> Since many tax refunds are issued by the IRS long before the tax form is fully scrutinized, some thieves have enough time to take the victim's refund money — and run.<sup>7</sup>

**Often, the victim doesn't even learn about the fraud until their own tax return is rejected** because a criminal has already submitted a return using the same Social Security number.<sup>8</sup>

## Know the Warning Signs of Tax-Related Identity Theft

The IRS advises taxpayers to stay alert to these common warning signs that they may be a victim of tax-related identity theft:

<b>A letter from the IRS inquiring about a suspicious tax return<sup>9</sup></b>	<b>A rejected e-filing because of previous filing using the same Social Security number</b>	<b>A tax transcript in the mail that the victim didn't request</b>
<b>An IRS notice that an online account in the victim's name has been created, accessed, or disabled, even though the victim didn't take any action</b>	<b>An IRS notice that the victim owes additional taxes, a refund offset, or has had collection actions taken against them for a year in which they did not file a tax return</b>	<b>IRS records that indicate wages from an employer that is unfamiliar to the victim</b>



Although the IRS has attempted to combat tax identity theft in recent years, the responsibility to protect your personal information begins with you — the taxpayer.<sup>1</sup>

### Why the IRS Advises Filing Taxes Early

In recent years, the IRS has recommended that taxpayers file as early as possible — and with good reason.<sup>9</sup>

The IRS accepts only one tax return per Social Security number, so **if a taxpayer can file their authentic tax return before a potential criminal can file their fraudulent one, they may be able to beat an identity thief to the punch.**<sup>10</sup> On the other hand, if a criminal succeeds in filing their fraudulent return first, it could take months for the victim to resolve issues associated with the return.<sup>4</sup>

In the race to beat a potential identity thief, some taxpayers may attempt to file an incomplete tax return with the intention of finishing it later, but that strategy could have negative consequences. The taxpayer could be charged penalties and interest for any delays in submitting a fully completed return, or multiple errors on a return could attract the attention of the IRS and trigger a second look or even an audit.<sup>11</sup>

Experts advise taxpayers to file as soon as they have collected all of the necessary documents, such as W-2s, 1099s, and mortgage interest statements.<sup>10</sup> And, of course, taxpayers should listen to the advice of their retained financial or tax professional.<sup>4</sup>

## The Dangers of IRS Phishing and Impersonation Scams

**One of the most common ways identity thieves get a victim's Social Security number and other information is through phishing campaigns,**<sup>1</sup> in which an attacker contacts the victim through email posing as a reputable organization or person.<sup>12</sup>

In fact, last year, the IRS reported a 60 percent increase in the number of tax-related phishing schemes.<sup>1</sup>

Scammers may create realistic-looking fraudulent messages that display the IRS logo or are designed to look like official communications from another organization, such as a tax software company.<sup>13</sup> The emails may trick victims into thinking they are eligible for a refund<sup>14</sup> or that they need to update their IRS e-filing status.<sup>13</sup> Fraudulent messages may even be sent to the victim's phone via text.

If the victim clicks on the link, they may unknowingly be sending their personal or financial information directly to the criminals via a fake website, or their computer may be infected with malware that can be used by criminals to access files or track keystrokes.





## The Most Pervasive Impersonation Scam in the History of the IRS

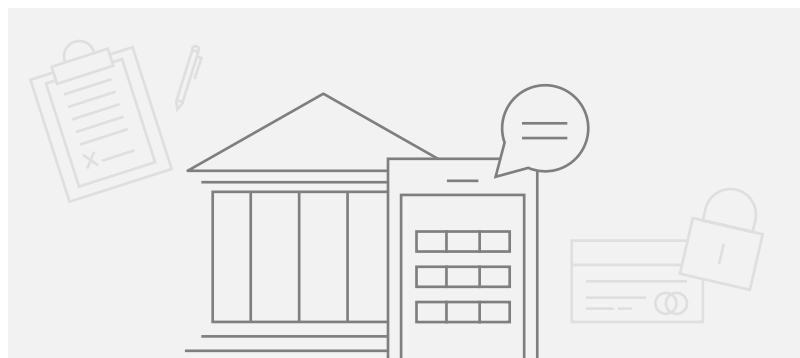
A sophisticated impersonation scam has hit some US taxpayers hard in recent years.<sup>13</sup>

The Treasury Inspector General for Tax Administration (TIGTA) has called the IRS impersonation scam “the largest, most pervasive impersonation scam in the history of the IRS.”<sup>15</sup> **More than 2.4 million people in the US have been targeted by IRS impersonators, with more than 14,700 victims losing a total of \$72.8 million.**

The impersonators call their victims claiming to work for the IRS or another law enforcement agency, even providing fake IRS badge numbers.<sup>13</sup> Victims are told that they owe taxes that must be paid immediately under the threat of arrest, suspension of a business or driver’s license, or deportation.

While many scammers go after vulnerable targets, such as elderly people and immigrants,<sup>16</sup> those who would appear less vulnerable are targeted — and fall for — the scam as well.<sup>17</sup>

While many scammers go after vulnerable targets, such as elderly people and immigrants,<sup>16</sup> those who would appear less vulnerable are targeted — and fall for — the scam as well.<sup>17</sup>



## It’s Crucial to Know How the IRS Typically Does — and Does Not — Contact Taxpayers

Perhaps one of the most important things for taxpayers to know is that **the IRS typically initiates contact with taxpayers through regular mail delivered by the United States Postal Service.**<sup>18</sup>

### According to the IRS, its agency will not:

- Call to demand immediate payment using a specific method, such as a prepaid debit card, gift card, or wire transfer<sup>13</sup>
- Threaten to bring in local police or other law enforcement<sup>19</sup>
- Demand payment without providing the opportunity to question or appeal the issue<sup>19</sup>
- Threaten a lawsuit<sup>20</sup>
- Leave pre-recorded, urgent messages asking for a call back<sup>18</sup>
- Send an unsolicited email to collect a pending refund or to update an account<sup>20</sup>
- Request any sensitive information online<sup>20</sup>
- Initiate contact by email, text message, or social media to request personal or financial information<sup>8</sup>
- Ask for credit or debit card numbers over the phone<sup>13</sup>

In recent years, the IRS began using a third-party debt collector to contact taxpayers regarding back taxes.<sup>15</sup> However, by law, both the IRS and the private debt collector will notify the taxpayer by mail first.





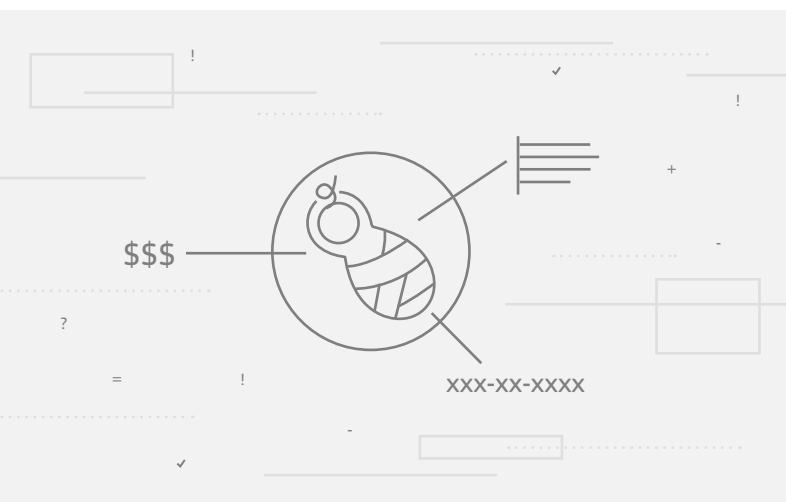
## Tax Identity Theft and Children

Even children can be vulnerable to tax-related identity theft. According to reports, cybercriminals have posted advertisements on the dark web selling children's identities,<sup>21</sup> and, in some cases, **the stolen data is being promoted for the purpose of committing tax fraud.**<sup>22</sup>

In one instance, criminals advertised data for sale called "infant fullz," encouraging potential buyers to purchase before tax season.<sup>22</sup> (The term 'fullz' is cybercriminal slang for a full identity kit — essentially everything a thief needs to steal an identity, such as name, address, Social Security number, and date of birth.)

What's the upside for a criminal claiming a dependent as their own? Cybercriminals can purchase an infant's data set for \$300 worth of bitcoin<sup>23</sup> in some cases compared to the \$1,000 a thief could potentially gain by claiming a dependent on a fraudulent tax return.<sup>7</sup>

Cybercriminals can purchase an infant's data set for \$300 worth of bitcoin<sup>23</sup> in some cases compared to the \$1,000 a thief could potentially gain by claiming a dependent on a fraudulent tax return.<sup>7</sup>



### Dependents and Shared Custody

It's common for blended families to unintentionally claim the same child as a dependent, and similar confusion can occur with siblings who claim a parent they care for as a dependent.<sup>24</sup>

**According to the IRS, an individual may be a dependent of only one taxpayer for a tax year, even if child custody is shared.**<sup>25</sup> The IRS provides tie-breaker rules in the form of an online tool to help taxpayers determine who can claim a dependent.<sup>26</sup>

# Steps to Better Protect Against Tax-Related Identity Theft

The good news is that there are preventative steps you can take to help better protect yourself and your loved ones from tax-related identity theft.

## Protect Yourself Before Tax Season Begins and Year-Round

- **Consider filing your tax return as early as possible.** One of the best ways to thwart identity thieves is to file your taxes as soon as possible.<sup>27</sup> This can give criminals a smaller window of time to successfully file a tax return in your name.
- **Learn to recognize and avoid IRS impersonations.** Avoid phishing emails, phone calls, and texts from criminals posing as legitimate organizations, such as banks, credit card companies, the IRS, and other government organizations.<sup>5</sup> Never click on links or download attachments from unknown or suspicious emails.
- **Defend devices and data.** Since many taxpayers now file online or store financial information on their computers, it is vitally important to keep computer and device security up-to-date.<sup>28</sup> Consider using security software with firewall and antivirus protections, and ensure the security software is functioning and can automatically update.<sup>5</sup> Encrypt sensitive files such as tax records stored on the computer. Use strong passwords — even passphrases — to protect personal accounts and sensitive files.<sup>1</sup> Computers used to store important tax documents should not be used by children or others who might expose the computer to unrestricted web browsing or install peer-to-peer software.<sup>28</sup>

## Choose Your Tax Preparer Wisely

- **Select a trusted tax preparer, if you use one.** If you plan to hire a tax preparer, do your research to ensure they are competent and ethical.<sup>29</sup> Investigate tax preparation companies, especially those located in new or seasonal offices, with the Better Business Bureau.<sup>28</sup> The Identity Theft Resource Center (ITRC) recommends asking potential tax preparers these questions: how information will be stored and encrypted, what computer security software is used, who has access to the information, whether or not the tax preparer has undergone a background screening, and how many years the tax preparer has worked for the company. Be especially wary of online tax preparers, as it could be a scam to gather your Social Security number and financial information.

- **Ask your tax preparer about his or her own security measures.** Tax preparers have increasingly become targets for cybercriminals looking for data on potential victims.<sup>1</sup> Ask your tax preparer how they protect client information and what their policies are for physical and electronic file storage. Ideally, they should have strict policies regarding the storage of client data as well as the deletion of files after their use.

## Deliver and Store Your Tax Return Securely

- **Protect physical documents used to prepare your return.** Law enforcement has reported increases in vehicle break-ins to steal documents that can be used to commit identity theft.<sup>28</sup> Keep sensitive personal information and documents safe during and after the filing process, and safely store or shred once no longer needed.<sup>29</sup> At your home or office, consider storing all tax documents and paperwork in a safe, locked location.<sup>28</sup> Since identity theft often requires access to personal information, keep in mind that the perpetrator could be a family member, friend, or caregiver.<sup>30</sup>
- **Be cautious with your e-filed or mailed return.** Once your return has been e-filed, save the file to a CD or flash drive and remove the information from your hard drive.<sup>28</sup> Store the CD or flash drive in a lock box or safe. If you mail your tax return, take it directly to a drop box located inside the post office, or if you have to use an outdoor drop box, it's best to deliver the package just before the last pick-up of the day. Don't leave tax documents in an outgoing mailbox at work.
- **Don't send tax information over public Wi-Fi networks.** Under no circumstances should you send your tax return or personal information over public Wi-Fi networks, and only provide such data through encrypted and trusted websites.<sup>1</sup> If you are using a tax preparer, ask if they have a secure in-house network to share confidential tax documents.

## Take Appropriate Steps If You Have Been the Victim of a Data Breach

If you've been notified that you may have been a victim of a data breach, talk with that organization to learn what it is doing to help protect you.<sup>8</sup> However, data breach victims should only submit an Identity Theft Affidavit to the IRS at [IdentityTheft.gov](https://www.irs.gov/identitytheft) if their Social Security number has been compromised and an e-filed return was rejected as a duplicate, or if the IRS instructs them to file the form.



## What to Do If You Think You Are a Victim of Tax Identity Theft

**If you suspect that you are a victim of tax-related identity theft, the IRS and the Federal Trade Commission (FTC) recommend the following steps:<sup>8</sup>**

- Respond immediately to any IRS notice by calling the phone number provided.
- File an Identity Theft Affidavit (IRS Form 14039) electronically at [IdentityTheft.gov](https://www.irs.gov/identity-theft) if your e-filed return gets rejected because of an existing filing under your Social Security number, or if the IRS instructs you to do so. The FTC recommends downloading and storing a copy of the report for your own records.<sup>31</sup>
- Continue to pay your taxes and file your tax return, even if you have to submit your tax return by mail.<sup>8</sup> Be aware that reporting suspected tax identity theft to the IRS or FTC does NOT eliminate the need to pay taxes.<sup>31</sup>
- Consider requesting a redacted copy (one with certain information blacked-out) of the fraudulent return from the IRS.<sup>32</sup> The information could help you determine what details the thief may have about you and your family.
- Follow the FTC's advice<sup>8</sup> to consider placing a fraud alert,<sup>33</sup> an extended fraud alert, or a credit freeze.<sup>34</sup>
- Contact your financial institutions and close any financial or credit accounts opened without your permission or tampered with by identity thieves.<sup>8</sup>

**If you suspect that you have been targeted by an IRS impersonator, the IRS provides the following advice to taxpayers:<sup>18</sup>**

- If you have no reason to think you owe taxes, hang up immediately and report the incident to the US Treasury Inspector General for Tax Administration (TIGTA) on their IRS Impersonation Scam Reporting ([www.treasury.gov/tigta/contact\\_report\\_scam.shtml](https://www.treasury.gov/tigta/contact_report_scam.shtml)) page and to the FTC through their FTC Complaint Assistant ([www.ftccomplaintassistant.gov](https://www.ftccomplaintassistant.gov)) page.
- If you are concerned you may owe taxes, review your tax account information online on the official website of the IRS, and call the number on the written billing notice, or contact the IRS at 800-829-1040.

## Additional Resources on Tax-Related Identity Theft

- The IRS provides many resources for individual taxpayers including a Taxpayer Guide to Identity Theft ([www.irs.gov/newsroom/taxpayer-guide-to-identity-theft](https://www.irs.gov/newsroom/taxpayer-guide-to-identity-theft)) and the web page IRS Identity Theft Assistance: How It Works ([www.irs.gov/individuals/how-irs-id-theft-victim-assistance-works](https://www.irs.gov/individuals/how-irs-id-theft-victim-assistance-works)).
- The FTC offers extensive information on their website [IdentityTheft.gov](https://www.ftc.gov/identity-theft), including a portal to report identity theft and create a recovery plan.
- Tax-related identity theft can also impact tax professionals and businesses. The IRS provides Identity Theft Information for both of these groups ([www.irs.gov/identity-theft-fraud-scams/identity-theft-information-for-tax-professionals](https://www.irs.gov/identity-theft-fraud-scams/identity-theft-information-for-tax-professionals)) and an Identity Theft Guide for Business, Partnerships, and Estate and Trusts ([www.irs.gov/individuals/identity-theft-guide-for-business-partnerships-and-estate-and-trusts](https://www.irs.gov/individuals/identity-theft-guide-for-business-partnerships-and-estate-and-trusts)).



**If you become a victim of identity theft, you don't have to face it alone. ID Watchdog is here for you.**

# Sources Cited

- <sup>1</sup>CNBC, "4 Tips to Protect Yourself Against Tax Return Fraud This Year" ([www.cnbc.com/2019/03/11/4-tips-to-protect-yourself-against-tax-return-fraud-this-year.html](http://www.cnbc.com/2019/03/11/4-tips-to-protect-yourself-against-tax-return-fraud-this-year.html))
- <sup>2</sup>Internal Revenue Service, "Key IRS Indicators Continue Dramatic Decline in 2017; Security Summit Marks 2017 Progress Against Identity Theft" ([www.irs.gov/newsroom/key-irs-identity-theft-indicators-continue-dramatic-decline-in-2017-security-summit-marks-2017-progress-against-identity-theft](http://www.irs.gov/newsroom/key-irs-identity-theft-indicators-continue-dramatic-decline-in-2017-security-summit-marks-2017-progress-against-identity-theft))
- <sup>3</sup>Federal Trade Commission, "Fight Back Against Identity Theft" ([www.consumer.ftc.gov/blog/2019/01/fight-back-against-tax-identity-theft](http://www.consumer.ftc.gov/blog/2019/01/fight-back-against-tax-identity-theft))
- <sup>4</sup>Investopedia, "Reasons to File an Early Tax Return" ([www.investopedia.com/taxes/file-early-tax-return/](http://www.investopedia.com/taxes/file-early-tax-return/))
- <sup>5</sup>Internal Revenue Service, "Identity Theft Remains on IRS' 'Dirty Dozen' List Despite Progress" ([www.irs.gov/newsroom/identity-theft-remains-on-irs-dirty-dozen-list-despite-progress](http://www.irs.gov/newsroom/identity-theft-remains-on-irs-dirty-dozen-list-despite-progress))
- <sup>6</sup>Identity Theft Resource Center, "The How and Why of Tax Identity Theft" ([www.idtheftcenter.org/the-how-and-why-of-tax-identity-theft/](http://www.idtheftcenter.org/the-how-and-why-of-tax-identity-theft/))
- <sup>7</sup>Consumer Reports, "Why Child Identity Theft Is a Growing Concern During Tax Season" ([www.consumerreports.org/identity-theft/why-child-identity-theft-is-a-growing-concern-during-tax-season/](http://www.consumerreports.org/identity-theft/why-child-identity-theft-is-a-growing-concern-during-tax-season/))
- <sup>8</sup>Internal Revenue Service, "Taxpayer Guide to Identity Theft" ([www.irs.gov/newsroom/taxpayer-guide-to-identity-theft](http://www.irs.gov/newsroom/taxpayer-guide-to-identity-theft))
- <sup>9</sup>Consumer Reports, "4 Reasons to File Taxes Early and Electronically, Especially This Year" ([www.consumerreports.org/taxes/reasons-to-file-taxes-early/](http://www.consumerreports.org/taxes/reasons-to-file-taxes-early/))
- <sup>10</sup>USA Today, "How Soon Can You File your Tax Return? Why Should You File ASAP?" (<https://www.usatoday.com/story/money/taxes/2018/01/28/how-soon-can-you-file-your-tax-return-why-should-you-file-asap/109462220/>)
- <sup>11</sup>Forbes, "Five Things You Need to Know About Identity Theft and Tax Returns" ([www.forbes.com/sites/kellyphillips/2018/02/02/five-things-you-need-to-know-about-identity-theft-and-tax-returns/#671ff27131ca](http://www.forbes.com/sites/kellyphillips/2018/02/02/five-things-you-need-to-know-about-identity-theft-and-tax-returns/#671ff27131ca))
- <sup>12</sup>TechTarget, "Definition: Phishing" ([searchsecurity.techtarget.com/definition/phishing](http://searchsecurity.techtarget.com/definition/phishing))
- <sup>13</sup>Internal Revenue Service, "Tax Scams/Consumer Alerts" ([www.irs.gov/newsroom/tax-scams-consumer-alerts](http://www.irs.gov/newsroom/tax-scams-consumer-alerts))
- <sup>14</sup>Internal Revenue Service, "Sample of a Phishing E-mail" ([www.irs.gov/pub/irs-utl/phishing\\_email.pdf](http://www.irs.gov/pub/irs-utl/phishing_email.pdf))
- <sup>15</sup>United States Senate Special Commission on Aging, "Fighting Fraud: Senate Aging Committee Identifies Top 10 Scams Targeting Our Nation's Seniors" ([www.collins.senate.gov/sites/default/files/2019%20Fraud%20Book.pdf](http://www.collins.senate.gov/sites/default/files/2019%20Fraud%20Book.pdf))
- <sup>16</sup>The New York Times, "U.S. Breaks Up Vast IRS Phone Scam" ([www.nytimes.com/2018/07/23/business/irs-phone-scams-jeff-sessions.html?module=inline](http://www.nytimes.com/2018/07/23/business/irs-phone-scams-jeff-sessions.html?module=inline))
- <sup>17</sup>ABC WXYZ-TV Detroit Channel 7, "Fenton Woman Falls Victim to IRS Impersonation Scam" ([www.youtube.com/watch?v=bOy9-P1JFNo](http://www.youtube.com/watch?v=bOy9-P1JFNo))
- <sup>18</sup>Internal Revenue Service, "IRS Continues Warning on Impersonation Scams; Reminds People to Remain Alert to Other Scams, Schemes This Summer" ([www.irs.gov/newsroom/irs-continues-warning-on-impersonation-scams-reminds-people-to-remain-alert-to-other-scams-schemes-this-summer](http://www.irs.gov/newsroom/irs-continues-warning-on-impersonation-scams-reminds-people-to-remain-alert-to-other-scams-schemes-this-summer))
- <sup>19</sup>Internal Revenue Service, "How To Know It's Really The IRS Calling or Knocking on Your Door" ([www.irs.gov/newsroom/how-to-know-its-really-the-irs-calling-or-knocking-on-your-door](http://www.irs.gov/newsroom/how-to-know-its-really-the-irs-calling-or-knocking-on-your-door))
- <sup>20</sup>Internal Revenue Service, "Taxes. Security. Together." ([www.irs.gov/pub/irs-pdf/p4524.pdf](http://www.irs.gov/pub/irs-pdf/p4524.pdf))
- <sup>21</sup>ZDNet, "The Latest Dark Web Cyber-Criminal Trend: Selling Children's Personal Data" ([www.zdnet.com/article/the-latest-dark-web-cyber-criminal-trend-selling-childrens-personal-data/?tag=TRE-03-10aaa6b&bhid=28547488407903236326816936236006](http://www.zdnet.com/article/the-latest-dark-web-cyber-criminal-trend-selling-childrens-personal-data/?tag=TRE-03-10aaa6b&bhid=28547488407903236326816936236006))
- <sup>22</sup>The Next Web, "The Worrying Trend of Children's Data Being Sold on the Dark Web" ([www.thenextweb.com/podium/2019/02/23/children-data-sold-the-dark-web/](http://www.thenextweb.com/podium/2019/02/23/children-data-sold-the-dark-web/))
- <sup>23</sup>CNN Business, "Infant Social Security Numbers Are For Sale on the Dark Web" ([www.money.cnn.com/2018/01/22/technology/infant-data-dark-web-identity-theft/index.html](http://www.money.cnn.com/2018/01/22/technology/infant-data-dark-web-identity-theft/index.html))
- <sup>24</sup>The Balance, "Audits for Determine Who Is Eligible to Claim a Dependent" ([www.thebalance.com/claiming-same-dependent-audit-risk-3193030](http://www.thebalance.com/claiming-same-dependent-audit-risk-3193030))
- <sup>25</sup>Internal Revenue Service, "Frequently Asked Questions: Dependents" ([www.irs.gov/faqs/filing-requirements-status-dependents/dependents/dependents-3](http://www.irs.gov/faqs/filing-requirements-status-dependents/dependents/dependents-3))
- <sup>26</sup>Internal Revenue Service, "Tie Breaker Rules" ([www.eitc.irs.gov/eitc-central/about-eitc/basic-qualifications/tie-breaker-rules/tie-breaker-rules](http://www.eitc.irs.gov/eitc-central/about-eitc/basic-qualifications/tie-breaker-rules/tie-breaker-rules))
- <sup>27</sup>Inc., "Identity Thieves Could Be Targeting Your Tax Returns. Here's How to Protect Yourself" ([www.inc.com/mediafeed/brian-acton/the-big-reason-to-file-your-taxes-in-january.html](http://www.inc.com/mediafeed/brian-acton/the-big-reason-to-file-your-taxes-in-january.html))
- <sup>28</sup>Identity Theft Resource Center, "Tax Time Tips" ([www.idtheftcenter.org/knowledge-base/tax-time-tips/](http://www.idtheftcenter.org/knowledge-base/tax-time-tips/))
- <sup>29</sup>New York State Department of Taxation and Finance, "Five Ways to Guard Against Identity Theft This Tax Season" ([www.tax.ny.gov/press/rel/2019/idtheftprotection021419.htm](http://www.tax.ny.gov/press/rel/2019/idtheftprotection021419.htm))
- <sup>30</sup>The Balance, "Dealing With Identity Theft by a Friend or Relative" ([www.thebalance.com/dealing-with-identity-theft-by-a-friend-or-relative-2386237](http://www.thebalance.com/dealing-with-identity-theft-by-a-friend-or-relative-2386237))
- <sup>31</sup>Federal Trade Commission, "A New Way to Report Tax Identity Theft" ([www.consumer.ftc.gov/blog/2018/04/new-way-report-tax-identity-theft](http://www.consumer.ftc.gov/blog/2018/04/new-way-report-tax-identity-theft))
- <sup>32</sup>Internal Revenue Service, "Instructions for Requesting Copy of Fraudulent Returns" ([www.irs.gov/individuals/instructions-for-requesting-copy-of-fraudulent-returns](http://www.irs.gov/individuals/instructions-for-requesting-copy-of-fraudulent-returns))
- <sup>33</sup>Federal Trade Commission, "Place a Fraud Alert" ([www.consumer.ftc.gov/articles/0275-place-fraud-alert](http://www.consumer.ftc.gov/articles/0275-place-fraud-alert))
- <sup>34</sup>Federal Trade Commission, "Extended Fraud Alerts and Credit Freezes" ([www.consumer.ftc.gov/articles/0279-extended-fraud-alerts-and-credit-freezes](http://www.consumer.ftc.gov/articles/0279-extended-fraud-alerts-and-credit-freezes))