



| Flash |

Financial Scams Threaten U.S. Tax Returns

F-2025-03-21a

Classification: TLP:CLEAR

Criticality: MEDIUM

Intelligence Requirements: Deep & Dark Web, Tax Fraud, Data Theft

March 21, 2025

Scope Note

ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were **identified prior to 9:00 AM EDT on March 21, 2025**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Flash | Financial Scams Threaten U.S. Tax Returns

| Key Findings

- As the April 15 deadline of the 2024–2025 U.S. tax season nears, ZeroFox Intelligence has identified a notable increase in financial fraud-related activity seeking to exploit the spike in use of government services such as the Internal Revenue Service (IRS) and private financial services.
- Historically, the end of the U.S. tax season has been perceived as a lucrative targeting opportunity by financially motivated threat actors seeking to obtain compromised account credentials, personally identifiable information (PII), or personal financial information (PFI) to exploit tax return processes.
- Threat actors engaging in this activity deploy targeted social engineering schemes, malicious domains mimicking popular financial service platforms, and bespoke services available in deep and dark web (DDW) forums.
- Malicious activity targeting U.S. tax return processes and the associated PII and PFI is very likely to continue over the coming weeks. If users engaging with the IRS experience delays, there is a likely chance that they will continue to be targeted in the weeks following the April 15, 2025, tax filing deadline.

| Details

As the April 15 deadline of the 2024–2025 U.S. tax season nears, ZeroFox Intelligence has identified a notable increase in financial fraud-related activity seeking to exploit the spike in use of government services such as the IRS and private financial services.

Historically, the end of the U.S. tax season has been perceived as a lucrative targeting opportunity by financially motivated threat actors seeking to obtain compromised account credentials, PII, or PFI to exploit tax return processes. To accomplish this, threat actors deploy targeted social engineering schemes, malicious domains mimicking popular financial service platforms, and bespoke services available in DDW forums.

Amid the 2024–2025 tax filing season, approximately 7 percent of IRS staff have reportedly been made redundant due to initiatives of the current U.S. presidential administration.¹ It is unclear the extent to which reduced staff will lead to less-secure tax return infrastructure or hinder the IRS's protection of customer information. However, any delays in IRS processes will afford threat actors a longer window of opportunity in which to conduct malicious activity. Delays are also likely to increase user frustration and stress—particularly if compounded by a lack of clarity or the simultaneous threat of punitive action.² This would likely result in higher interaction with malicious services masquerading as timely and convenient solutions.

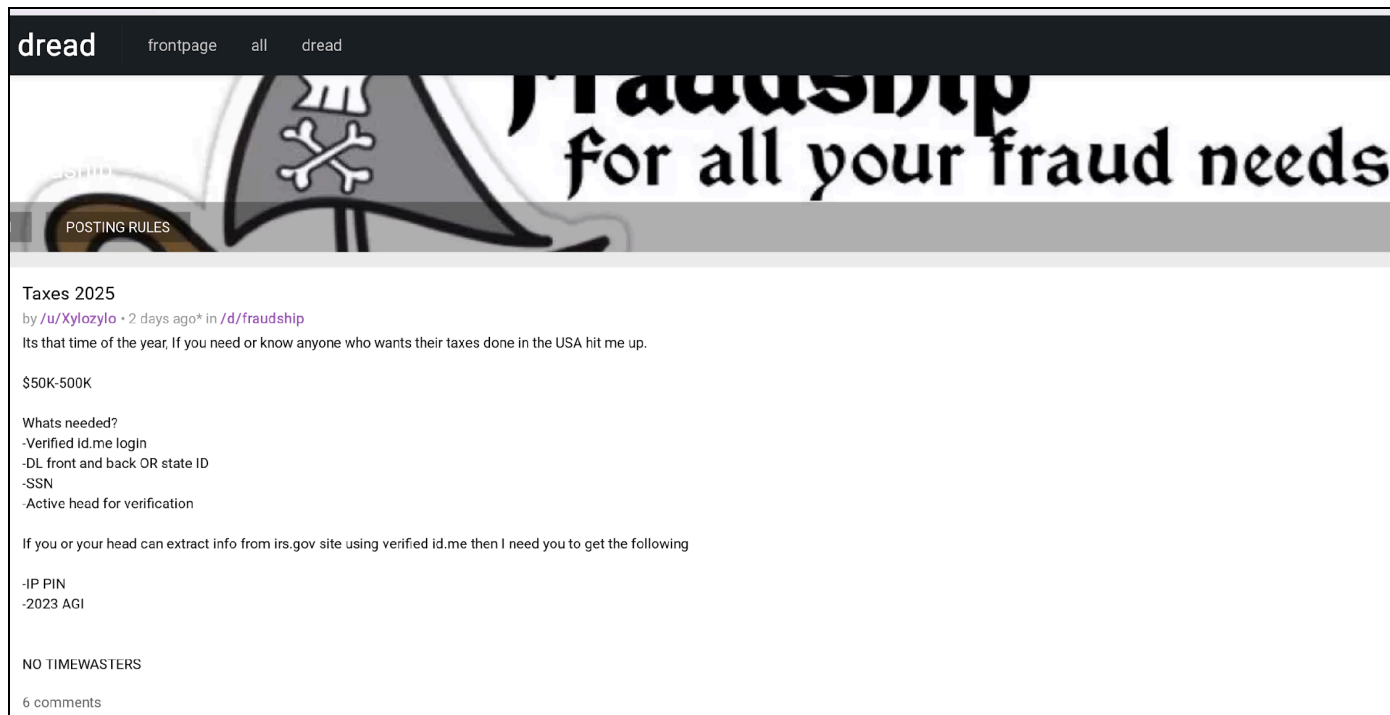
| Malicious Dark Web Services

On March 9, 2025, an actor named “Xylozylo” posted in the Fraudship section of the dark web forum Dread, advertising fraudulent tax return services available for purchase. According to the post, Xylozylo can assist buyers seeking to submit fraudulent returns for incomes between USD 50,000 to USD 500,000, as long as they are able to provide a potential victim's:

- Verified id.me login credentials
- Driver license details (front and back) or other state-issued identification
- Social Security Number (SSN)

¹ [hXXps://apnews\[.\]com/article/irs-layoffs-trump-elon-musk-doge-df2b3c8d53ff9f2d276c8b29f8004dde](https://apnews.com/article/irs-layoffs-trump-elon-musk-doge-df2b3c8d53ff9f2d276c8b29f8004dde)

² [hXXps://www.credello\[.\]com/financial-resources/consumer-insights/tax-stress-return-survey/](https://www.credello.com/financial-resources/consumer-insights/tax-stress-return-survey/)



dread frontpage all dread

Fraudship for all your fraud needs

POSTING RULES

Taxes 2025
by /u/Xylozylo • 2 days ago* in /d/fraudship

Its that time of the year, If you need or know anyone who wants their taxes done in the USA hit me up.

\$50K-500K

Whats needed?

- Verified id.me login
- DL front and back OR state ID
- SSN
- Active head for verification

If you or your head can extract info from irs.gov site using verified id.me then I need you to get the following

- IP PIN
- 2023 AGI

NO TIMEWASTERS

6 comments

Advertisement by Xylozylo in Dread

Source: ZeroFox Intelligence

Xylozylo further specified that if buyers are able to provide information from the IRS website via a compromised id.me account, they need only provide the victim's identity protection (IP) PIN and their 2023 adjusted gross income (AGI) to proceed.

Another actor, "Fraudbay" (who claims to have personally filed over 3,000 fraudulent tax returns this season and to have sold 7,000 more) responded to the post stating that a verified id.me account is not necessary. Instead, Fraudbay advises that fraudulent tax returns can be submitted via third-party services such as TurboTax or H&R Block, allegedly circumventing the need for id.me verification.

- ZeroFox cannot confirm if Fraudbay's claims are legitimate, as verification requirements likely vary by use case. However, the use of such third parties very likely reduces the extent to which claimants are required to interact with IRS services, which incorporates id.me verification into its Know Your Customer (KYC) security protocols.

Fraudbay also offers their own malicious financial services in the dark web marketplace BlackOps. One such service observed by ZeroFox is the advertisement of illegitimate IRS tax documents—including the U.S. Individual Income Tax Return (1040) and the Wage and Tax Statement (W2). According to the listing, the package consists of the following information:

- All information required for filing a tax return “this season”
- Driver license (front and back)
- AGI from the previous year
- Date of Birth (DoB)
- Utility bill scans (available as an extra purchase)



2025 W2 1040 DL SCANS - AGI AND DOB INCLUDED

 5.00 Sold: 0

\$90.00 (0.44814 XMR)

Escrow (14)

Product summary

2025 Tax Season W2 and 1040 forms filled by companies for their employees. Contains all info required for filing tax returns this season PLUS DL SCANS BACK AND FRONT. Previous year AGI and DOB included. Utility scans and SELFIE WITH DL are available for extra. Bulk discounts available and starting from 10 pieces.

Quantity

1

Buy Now

Add to Cart

Product description

About this vendor

Terms of Services (ToS)

2025 Tax Season W2 and 1040 forms filled by companies for their employees. Contains all info required for filing tax returns this season PLUS DL SCANS BACK AND FRONT. Previous year AGI and DOB included. Utility scans and SELFIE WITH DL are available for extra.

Bulk discounts available and starting from 10 pieces.

Advertisement by Fraudbay in BlackOps

Source: ZeroFox Intelligence

The PII and PFI used to populate these forms has very likely been obtained through previous data breaches implicating government departments or one of the many third-party accountancy firms that are widely used by the U.S. populace in preparing and filing tax returns.³

³ [hXXps://www.irs\[.\]gov/newsroom/filing-season-statistics-for-week-ending-jan-31-2025](https://www.irs.gov/newsroom/filing-season-statistics-for-week-ending-jan-31-2025)

- ZeroFox Intelligence is unable to confirm the proportion of scams such as these that lead to the payout of fraudulent tax returns, though their popularity within DDW forums in the weeks approaching April 15 indicate that a significant number of cyber threat actors consider it lucrative.

Fraudbay's services are priced at USD 90 for a "set". While it is unclear what exactly this consists of, ZeroFox observed similar offerings advertised in the dark web forum xss for USD 20 prior to the April 2024 tax filing deadline. While both of these prices are relatively low, it is very likely that threat actors engaging in this activity often do so en masse to enhance the likelihood of success.

In addition to tax return fraud, stolen PII and PFI is also leveraged to conduct various other malicious tax-related schemes:

- Threat actors use stolen PII to conduct phishing and spear-phishing campaigns, often masquerading as representatives of the IRS. These attacks are intended to trick the victim into providing personal details such as banking or IP PIN information, which can aid in subsequent attacks. Malicious links can also be used to direct the victim to fake web pages that are able to deliver malware and harvest credentials.
- Threat actors attempt to collect false tax debt using stolen PII to increase authenticity while imitating employees of either the IRS or an external debt collection agency. These attacks often leverage several social engineering techniques to encourage the victim's cooperation.
- Fake IRS letters claim that additional PII is needed in order to process an unclaimed tax refund. However, the information provided by the victim assists the threat actor in submitting fraudulent tax returns.

Malicious activity targeting U.S. tax return processes and the associated PII and PFI is very likely to continue over the coming weeks. If users engaging with the IRS experience significant delays, there is a likely chance that they will continue to be targeted in the weeks following the April 15, 2025, deadline. In such a case, some threat actors will likely pivot their tactics, techniques, and procedures (TTPs) toward the targeting of affected individuals, leveraging phishing communications to deliver malicious services masquerading as timely solutions.

Recommendations

- Individuals with an SSN or an Individual Taxpayer Identification number (ITIN) should register annually for an IP PIN using the following address:
 - [hXXps://www.irs\[.\]gov/identity-theft-fraud-scams/get-an-identity-protection-pin](https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin)
- Maintain awareness of contemporary threats by following IRS guidance:
 - [hXXps://www.irs\[.\]gov/newsroom/dirty-dozen-tax-scams-for-2025-irs-warns-taxpayers-to-watch-out-for-dangerous-threats](https://www.irs.gov/newsroom/dirty-dozen-tax-scams-for-2025-irs-warns-taxpayers-to-watch-out-for-dangerous-threats)
- Being implicated in a data breach could be the first step toward PII being leveraged to conduct tax fraud. In such a case, the individual should consider placing a “Fraud Alert” on their credit file.
- Suspected scamming or identity theft activity should be reported using [.]gov tools found here:
 - [hXXps://www.usa\[.\]gov/where-report-scams](https://www.usa[.]gov/where-report-scams)
 - [hXXps://www.irs\[.\]gov/pub/irs-pdf/f14039.pdf](https://www.irs.gov/pub/irs-pdf/f14039.pdf)
- Individuals should scrutinize correspondence purporting to be from the IRS or third-party services, particularly if received via unusual communication channels or if found to contain spelling and grammatical errors. If in doubt, further personal information should not be disclosed, and the request should be verified through official communications.
- Individuals using third-party tax return preparation services should ensure that documentation is appropriately signed upon completion.
- Organizations and individuals should ensure passwords are secure, unique credentials are used, and multi-factor authentication (MFA) is implemented to ensure the security of their personal information.

Appendix A: Traffic Light Protocol for Information Dissemination

	Red	Amber
WHEN SHOULD IT BE USED?	Sources may use TLP:RED when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.	Sources may use TLP:AMBER when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.
HOW MAY IT BE SHARED?	Recipients may NOT share TLP:RED with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.	Recipients may ONLY share TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm. Note that TLP:AMBER+STRICT restricts sharing to the organization only.
	Green	Clear
WHEN SHOULD IT BE USED?	Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.	Sources may use TLP:CLEAR when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.
HOW MAY IT BE SHARED?	Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community but not via publicly accessible channels.	Recipients may share TLP:CLEAR information without restriction, subject to copyright controls.

| Appendix B: ZeroFox Intelligence Probability Scale

All ZeroFox intelligence products leverage probabilistic assessment language in analytic judgments. Qualitative statements used in these judgments refer to associated probability ranges, which state the likelihood of occurrence of an event or development. Ranges are used to avoid a false impression of accuracy. This scale is a standard that aligns with how readers should interpret such terms.

Almost No Chance	Very Unlikely	Unlikely	Roughly Even Chance	Likely	Very Likely	Almost Certain
1-5%	5-20%	20-45%	45-55%	55-80%	80-95%	95-99%