ZEROFOX INTELLIGENCE

# Brief

## The Underground Economist: Volume 5, Issue 25

B-2025-12-18b

Classification: TLP:CLEAR

Criticality: LOW

Intelligence Requirements: Deep and Dark Web, Threat Actor, Data Breach

December 18, 2025

*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 10:30 AM (EST) on December 18, 2025; per cyber hygiene best practices, caution is advised when clicking on any third-party links.*

# Brief The Underground Economist: Volume 5, Issue 25

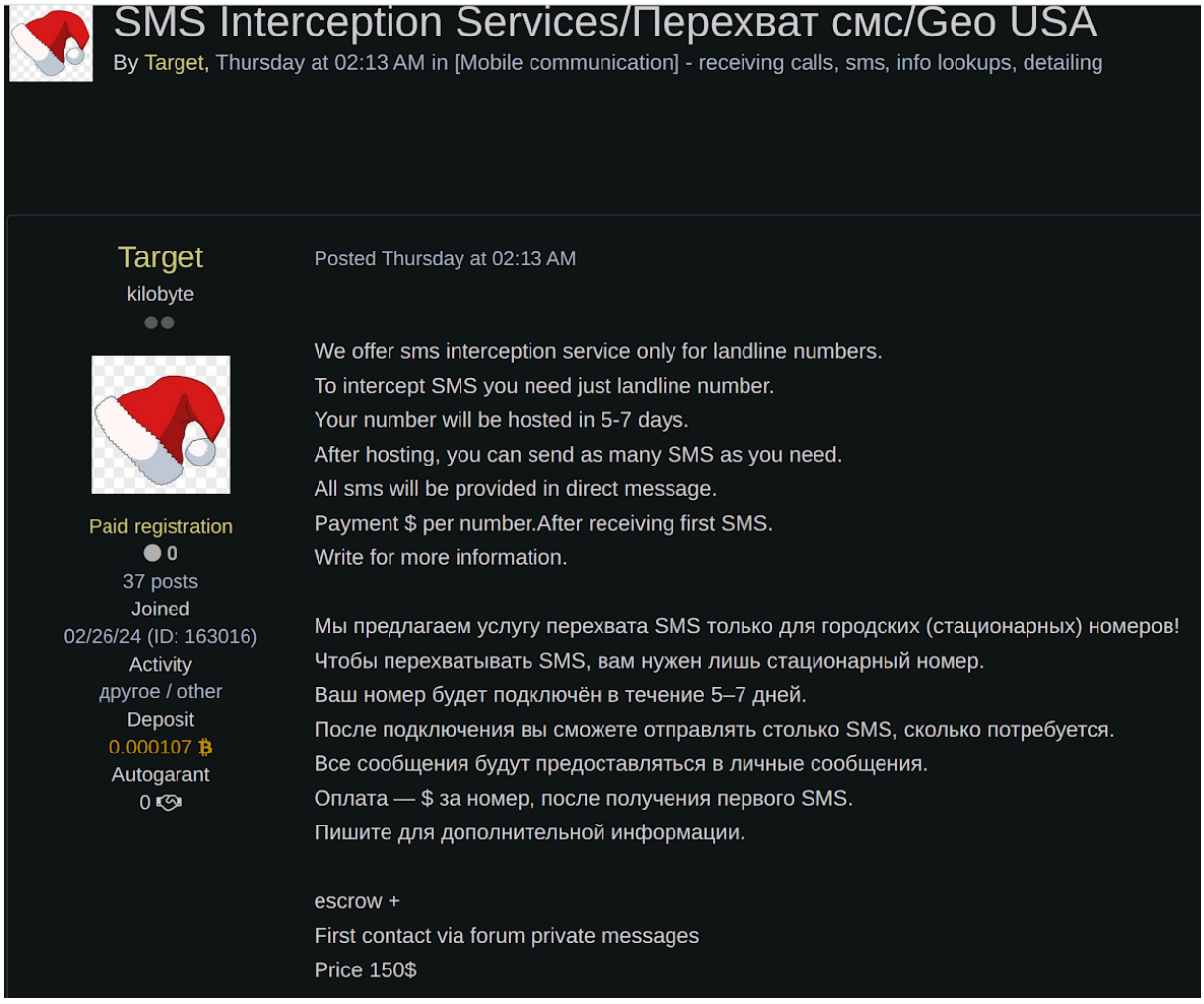
## Landline SMS Interception Service Advertised on Exploit

On December 11, 2025, an established but unvetted threat actor known as "Target" advertised an SMS interception as a service on the dark web forum Exploit. In the post, the actor shared all terms and requirements for providing SMS interception upon request—including that the offer only works for U.S. landline numbers, and the hosting fee is USD 150 per number. As outlined by the actor, the process for buyers is as follows:

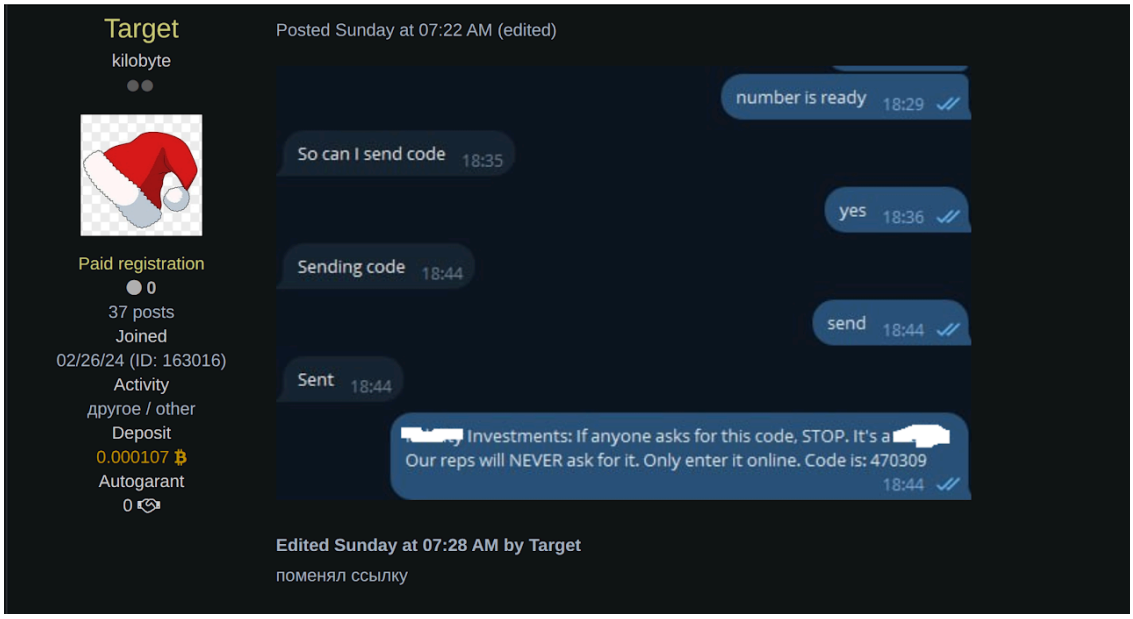
- The buyer provides the victim's landline number.
- The number will be hosted by the seller within five to seven days.
- Once hosted, the buyer will be able to send an unlimited number of SMS messages for one week.
- All SMS responses will be provided to the buyer via direct message.
- The buyer will be charged per number after receiving the first SMS.

Target provided no further details on how the SMS interception method works. Since the offer is relatively new, there is a roughly even chance the actor will add additional information to the post. However, Target shared a screenshot from a suspected Telegram chat with a potential client as proof of their SMS interception capabilities.

- The screenshot indicates that Target provided the buyer with an alleged SMS containing a one-time code intended to be used to log in to a compromised account likely associated with Fidelity Investments.




**Target's SMS interception offer on Exploit**
*Source: ZeroFox Intelligence*




**Alleged proof of service provided by Target**
*Source: ZeroFox Intelligence*

Target appears to have joined Exploit in February 2024; despite having contributed 37 posts to the forum, the actor lacks any positive or negative reputation. In response to the post, Target received a moderator warning on this offer stating that the actor is required to complete any transactions through escrow or middleman services.

- While the actor being on the forum for nearly two years would typically contribute towards Target's credibility, ZeroFox considers the actor untested due to their lack of reactions from Exploit's community.

There is a roughly even chance that Target's SMS interception service is legitimate; however, ZeroFox cannot determine the offer's credibility due to the actor's lack of reputation. If the service is legitimate, victims would very likely be at risk of account compromises, identity theft, and other forms of financial fraud.

## IRS Pension Data for Sale on DarkForums

On December 10, 2025, an actor on DarkForums using the name "Frenshyny" advertised a large database allegedly exfiltrated from the Internal Revenue Service (IRS). According to the post, the dataset contains information related to 401(k) benefit funds for 18 million Americans over the age of 65.

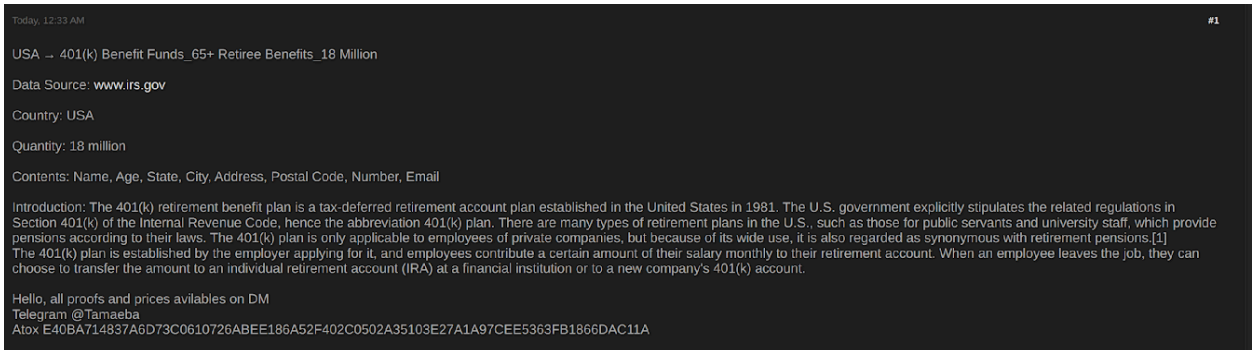
- The 401(k) is an American retirement savings plan that has been widely used in the United States since 1981, when the IRS first published regulations related to the Revenue Act of 1978.[1]

Frenshyny did not specify when the breach occurred in the post, but the size of the database being offered would likely make this the largest data breach in the history of the U.S. private pension sector if it is legitimate. The IRS has not made any statements confirming or denying the breach to date.

The information allegedly available in the database is extensive and, if confirmed, would almost certainly be used to conduct identity theft, elder fraud, financial account takeovers, or phishing campaigns targeting retirees. According to Frenshyny, the information on 18 million individuals includes:

- Name
- Age
- Full address
- Phone number
- Email address

[1] hXXps://www.cnbc[.]com/2017/01/04/a-brief-history-of-the-401k-which-changed-how-americans-retire.html




**Frenshyny's post on DarkForums**
*Source: ZeroFox Intelligence*

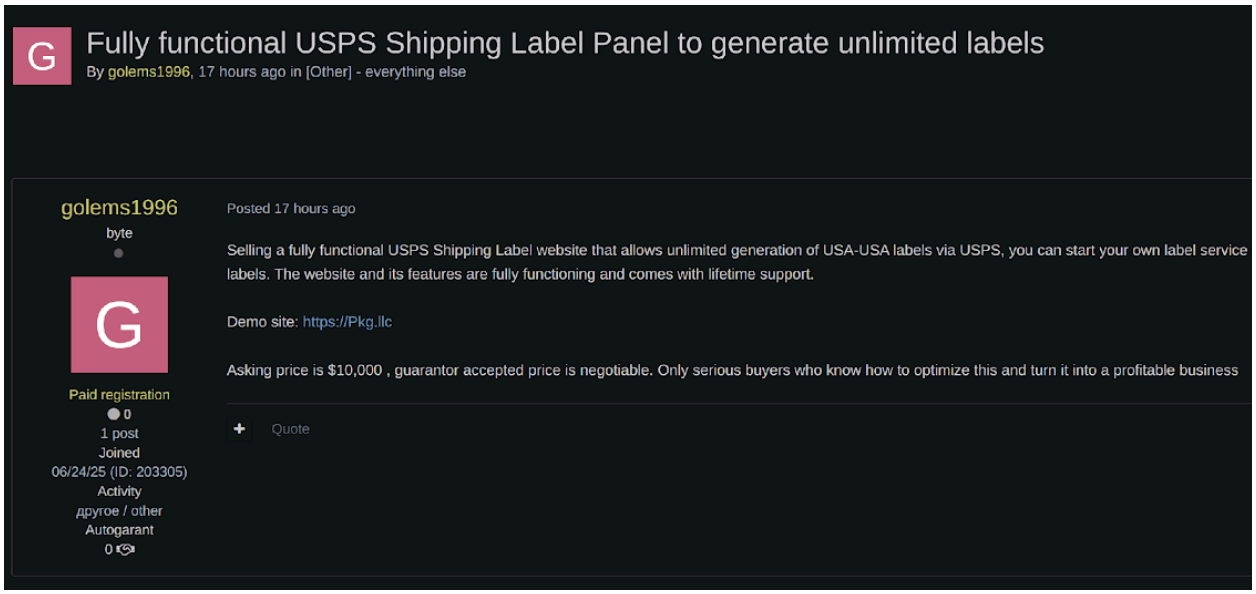
A IRS source origin would indicate a serious federal data compromise; however, such claims are often exaggerated or fabricated by threat actors to inflate the perceived value of a dataset. The post does highlight the growing threat cybercriminals pose to pension funds. ZeroFox assesses cyberattacks against pension programs around the globe are on the rise, likely because these funds typically contain large balances and extensive personal data on potential targets that can be used for financial theft, fraud, and other types of cybercrime.

## Exploit Actor Advertises Fake USPS Shipping Label-Generating Website

On December 9, 2025, a threat actor using the alias "golems1996" posted on the dark web forum Exploit, advertising the sale of a shipping label-generating website. Golems1996 claimed that the website, priced at USD 10,000, can generate "unlimited" U.S. Postal Service (USPS) domestic shipping labels and will come with lifetime support.

- Golems1996 joined Exploit in June 2025 and has not yet garnered a positive reputation, posting only once.
- At the time of writing, this post has not gained any traction from other Exploit members.
- USPS has reportedly observed a surge in fake USPS labels being widely abused, prompting inspectors to review shipments at USPS facilities and intercept packages bearing counterfeit postage. Since October 2024, USPS's efforts have

resulted in the seizure of counterfeit stamps worth USD 16.2 million and 358 voluntary discontinuance orders.[2]




**golems1996's Exploit post**

*Source: ZeroFox Intelligence*

The threat actor stated that they are willing to use a trusted "guarantor," which likely suggests an escrow service (a common practice on dark web forums to ensure payment and reduce risks of fraud). However, a guarantor does not validate the technical claims or long-term viability of the service.

It is likely that such a service would enable outcomes that include:

- Large-scale postal fraud
- Facilitation of criminal logistics
- Abuse in money laundering or reshipping schemes
- Increased risk of identity and address misuse
- Reputational and operational harm to USPS
- Broader exploitation attempts across related systems

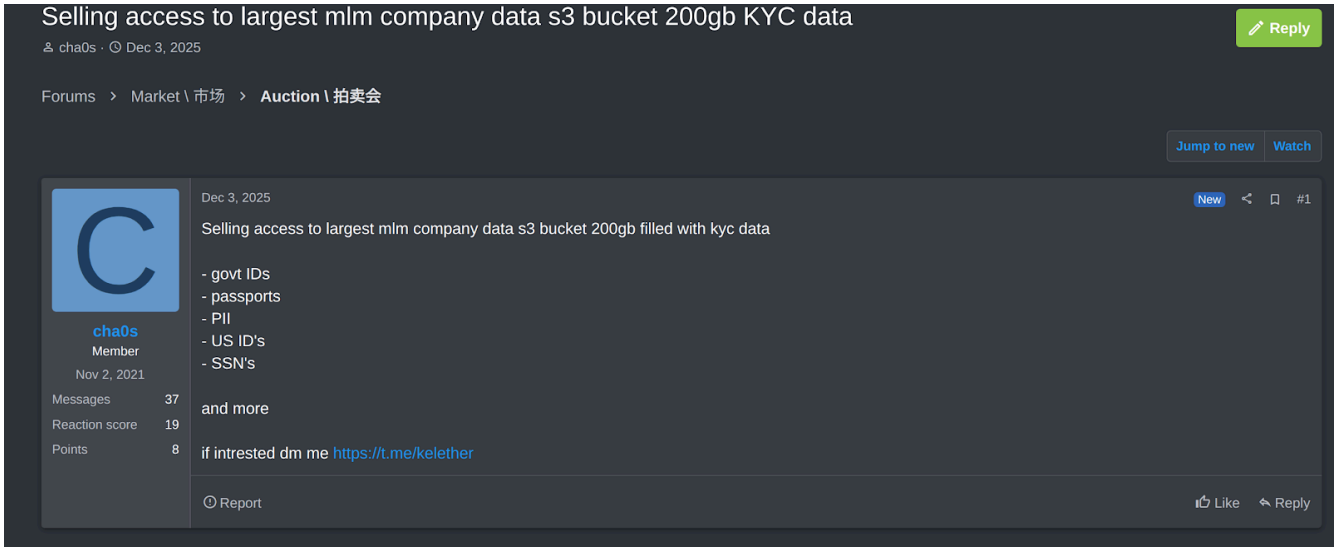
[2] hXXps://news.usps[.]com/2025/09/29/inspection-service-to-consumers-dont-fall-for-fake-stamp-schemes/

There is a roughly even chance that this advertisement will gain interest from potential buyers on the forum. This type of access will likely appeal to a range of financially motivated threat actors seeking to conduct an array of malicious activities, including social engineering campaigns.

## Access to Leading MLM Company Advertised for Sale on Dark Web Forum

On December 3, 2025, the actor "cha0s" posted on the dark web forum RAMP, advertising the sale of unauthorized access to the largest multi-level marketing (MLM) company in the world. According to the post, the price for the access would be disclosed privately via Telegram.

- As of the time of writing, the largest MLM based on revenue is the U.S.-based company Amway, which reportedly generated USD 7.4 billion in 2024.[3]
- Cha0s is an established threat actor on RAMP that joined the forum in November 2021 and has since established a positive reputation.




**cha0s's RAMP post**
*Source: ZeroFox Intelligence*

[3] hXXps://www.epixelmlmsoftware[.]com/blog/top-solid-100-mlm-companies-in-2018

According to cha0s, they had access to the unnamed company's simple storage service (S3) bucket, which allegedly contains 200 GB of filled data and know your customer (KYC) data. Cha0s claims the data includes the following:

- Government-issued IDs
- Passports
- Personally identifiable information (PII)—likely meaning names, addresses, emails, or phone numbers
- U.S. identification documents
- Social Security numbers

This advertisement will almost certainly garner interest from a host of potential buyers, given the type of access listed and the reputation of the seller. Threat actors could leverage the data advertised for multiple malicious activities, including opening mule accounts, applying for fraudulent loans, or using the information to obtain tax documents and commit fraud.

- Spikes in U.S. financial fraud are typical in January, when the window opens for taxpayers to file annual tax returns, and threat actors are known to use stolen information to file fake ones.

## Recommendations

- Develop a comprehensive incident response strategy.
- Deploy a holistic patch management process, and ensure all IT assets are patched with the latest software updates as quickly as possible.
- Adopt a Zero-Trust cybersecurity architecture based upon a principle of least privilege.
- Implement network segmentation to separate resources by sensitivity and/or function.
- Ensure critical, proprietary, or sensitive data is always backed up to secure, off-site, or cloud servers at least once per year—and ideally more frequently.
- Implement secure password policies, phishing-resistant multi-factor authentication (MFA), and unique credentials.
- Configure email servers to block emails with malicious indicators, and deploy authentication protocols to prevent spoofed emails.
- Proactively monitor for compromised accounts and credentials being brokered in deep and dark web (DDW) forums.
- Leverage cyber threat intelligence to inform the detection of relevant cyber threats and associated tactics, techniques, and procedures (TTPs).

# 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% |