Graphika

Vulnerability Vultures

How Scammers Entice Targets Via Impersonation and Fictional Financial Aid Offers

10.2025

Vulnerability Vultures

How Scammers Entice Targets Via Impersonation and Fictional Financial Aid Offers

Overview

Scams targeting vulnerable populations, especially older adults, remain a consistent feature of the online fraud landscape, according to public reporting and law enforcement agencies. In 2024, the FBI's Internet Crime Complaint Center (IC3) received its highest number of complaints from the 60-plus age group, whose losses totaled $4.8 billion – almost double the next greatest loss value. Similarly, 2024 data from the Federal Trade Commission shows that adults 70 years or older lose a significantly higher median dollar value to scams than those under 70.

Through our intelligence monitoring, Graphika regularly detects, tracks, and helps disrupt a wide array of scams on multiple online platforms. Working with industry partners at Meta, we've joined a campaign to raise public awareness about online scams. This report, released during Cybersecurity Awareness Month in the U.S., focuses on scammers targeting populations they see as especially lucrative or vulnerable, such as older adults.

Our findings aren't exhaustive, but rather a set of case studies illustrating how these types of scams attempt to engage, deceive, and defraud people of their money. We've selected the examples based on a combination of key attributes, including their relevance as scams targeting seemingly vulnerable communities, prevalence across internet platforms, and notable tactics, techniques, and procedures.

Key Findings

- The research presented here covers an international ecosystem of scams designed to exploit the reputation of trusted organizations to defraud online users. Based on public social media data, some scam accounts' operators appear to be based in Nigeria, South Asia, and the U.S. They're targeting individuals who may be especially susceptible to offers of physical or financial benefits: older adults and victims of previous scams.

- The scammers use major social media platforms to attract their targets, then redirect them to fraudulent websites or private messages to divulge financial details or sensitive personal data. The cross-platform structure of scam operations enables scalability, anonymity, and evasion of platform moderation measures.

- We consistently observed the scammers using inauthentic personas and manipulated media to impersonate trusted figures, institutions, and brands, such as the FBI or news organizations. By supporting the illusion with AI-generated audio, cloned websites, and reused authentic content, their accounts, posts, and messages attempt to simulate legitimacy and authority.
- The operations follow a recurring pattern we've seen across our scams work: build trust, usher targets off-platform, and extract personal or financial data through registration for non-existent relief programs or submission of complaint forms based on organizational trust. These schemes operate at a high volume of solicitation, often aided by identical and often short-lived ads, AI, automation, paid promotion, and disposable accounts that maintain persistence despite ongoing enforcement efforts.

Case Studies

Home Remodeling and Debt Relief Ads Target Older Adults

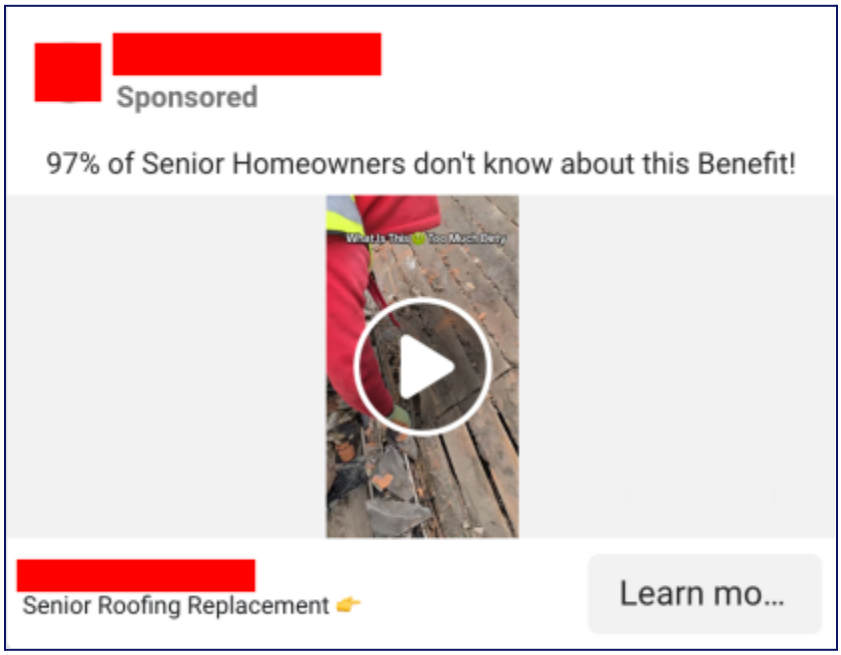
A network of at least 25 domains invited older adults to take advantage of nonexistent home renovation or debt relief offers. To drive traffic to these sites, scammers ran ads using fully and partially AI-generated content on Facebook, Google products, and YouTube. The ads primarily frame these offers as part of vague government efforts, including "Senior Roofing Initiative" or "Senior Bathroom Relief." The ads include videos that follow similar behavioral and content patterns, including:

- Presenting as a podcast interview of a senior homeowner discussing an unknown government initiative to help seniors remodel their homes or receive debt relief
- Presenting as a news report from a trusted news source about the nonexistent initiative
- Presenting footage of speakers on a stage talking to a large audience about the initiative
- Presenting generic home remodeling footage alongside an AI-generated voiceover in which the supposed homeowner discusses how they were able to remodel their home due to the initiative

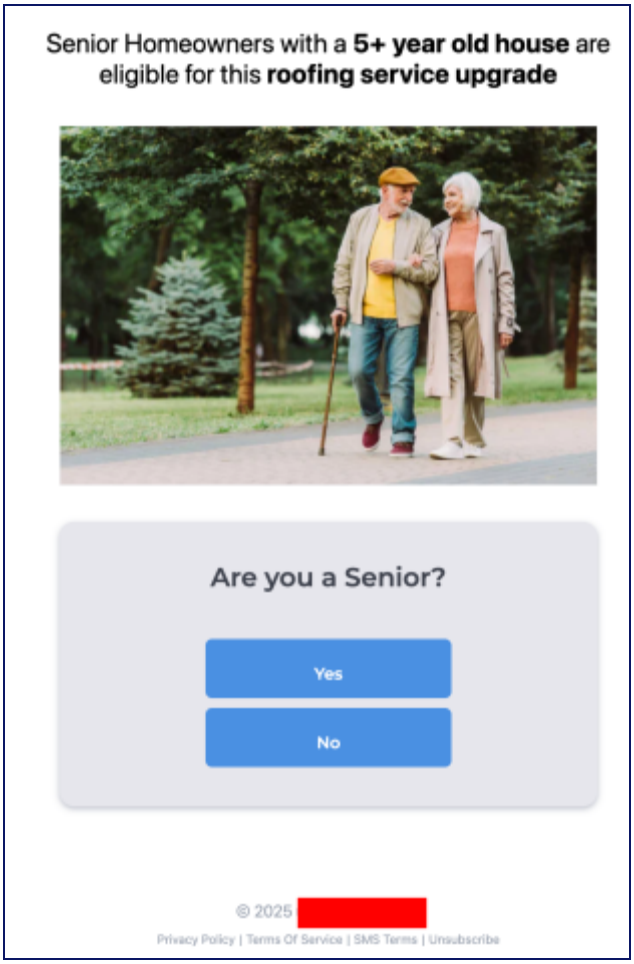
Many of the domains – which we linked through shared advertising ID codes, similar naming conventions, and repetitive site design – appear designed to harvest a user's personal information, including name, location, household debt, and desire for home renovations. Some publicly available comments on business review platforms suggest that scam target information is sold to legitimate contractor businesses as qualified leads. If accurate, this could lead to repeated calls and pressure to accept expensive renovation or debt relief services.

Several identified domains use logos of trusted business registries, review sites, and media outlets to imply these organizations' endorsement. However, we found no mention of these domains or the business names they display on any trusted business registry services we reviewed.

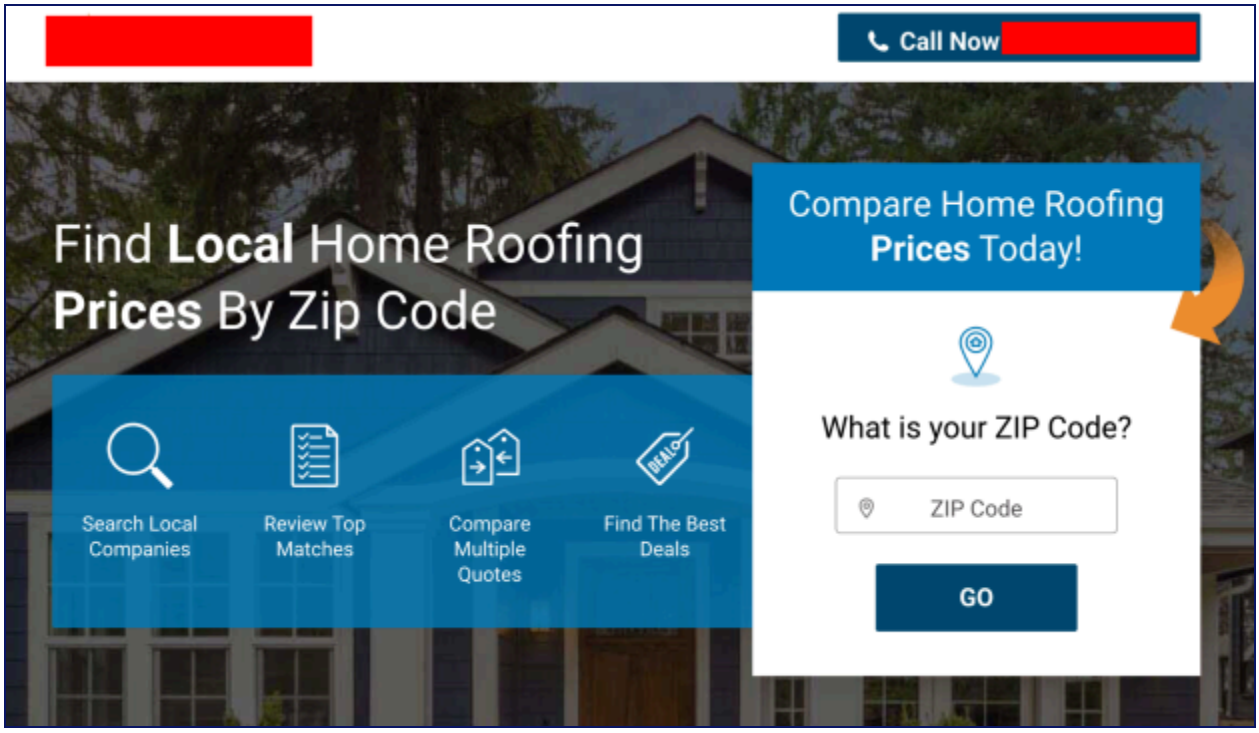
Across platforms, the engagement process is similar. A user is presented with one of the aforementioned ads offering home renovation or debt relief services that directs them to a domain. The domain landing pages all present a binary yes/no question – for example, "Are you a senior homeowner?" – but regardless of the chosen answer, the user is then funneled to a separate domain that requests a user's ZIP code and redirects them to a second site where they are invited to input other personal information.



A Facebook ad directing users to one of the information-harvesting domains. The ad includes a video showing home repair with an AI-generated voiceover, and a "Learn more" button leading to the site shown in the following image. Redactions added by Graphika.



One of the websites promising benefits for senior citizens, presenting a yes/no question that, regardless of what the user clicked, led to the site shown in the following image. Redaction added by Graphika.



A website presenting itself as a standalone business offering price comparisons, prompting the user to enter their ZIP code and click a button, which led to another website requesting more personal information. Redactions added by Graphika.

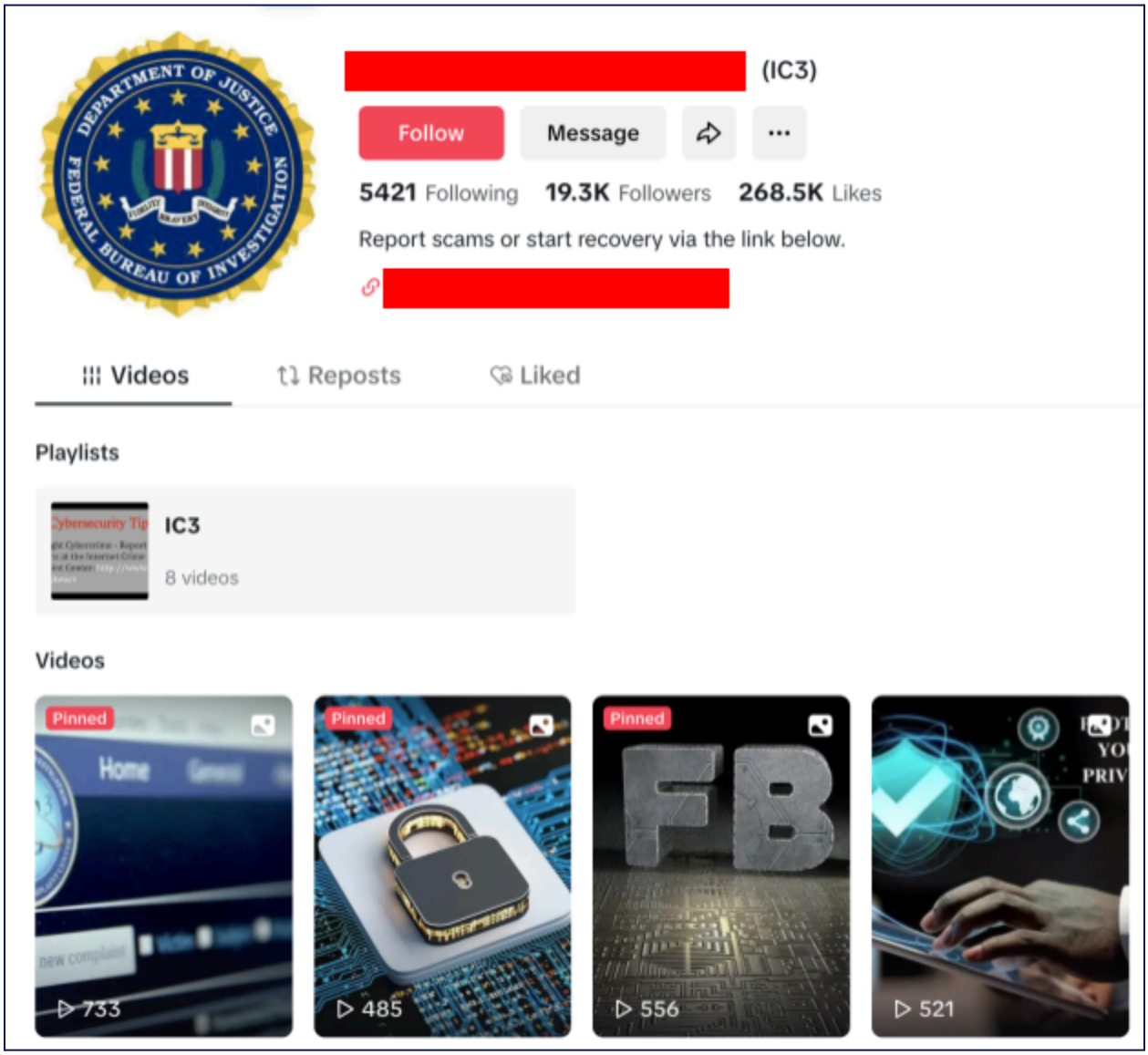
Fraudulent Fund Recovery Scam Impersonating FBI

We identified multiple websites mimicking the FBI's Internet Crime Complaint Center (IC3), including options for scam victims to file reports requiring personal and financial information. In this cross-platform, multi-language scam, malign actors use inauthentic accounts posing as IC3 across Facebook, Instagram, Telegram, Threads, TikTok, YouTube, and X. These accounts often include "IC3" in their handles and page titles, use official FBI insignia in profile photos and posts, and link to the authentic IC3 website in their posts or bios. They promise to help fraud victims recover lost funds, but instead redirect users into fraudulent schemes through private messages or visits to sites mimicking the official IC3 site. Open-source indicators suggest some inauthentic accounts' administrators are located in Nigeria and Southeast Asia.

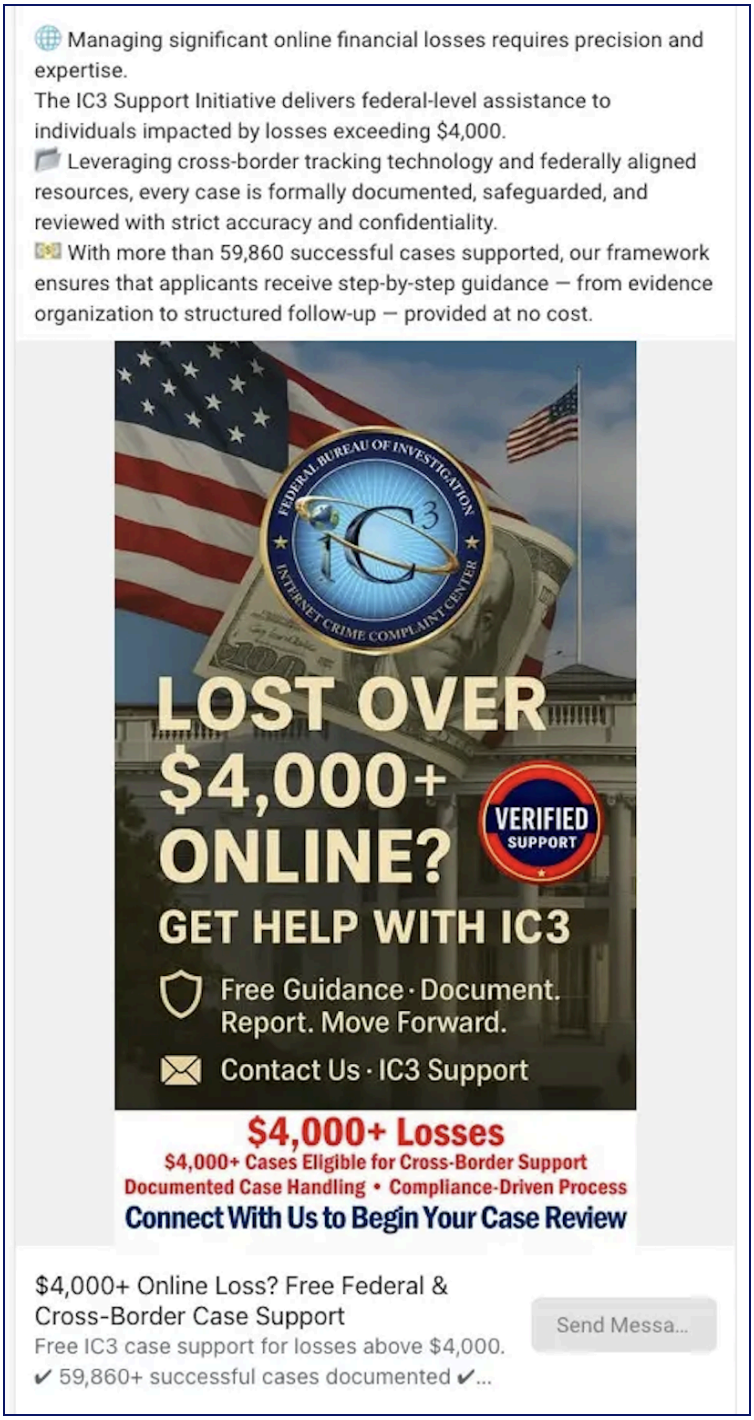
This scam attempts to exploit public trust in a U.S. law enforcement agency to deceive individuals who are already vulnerable after losing money to fraud. IC3's 2024 reporting shows that most of their complaints originate from the 60-plus age group, suggesting an enhanced risk for recovery schemes for this group. In September 2025, the FBI warned about a surge in IC3 impersonations targeting victims of online scams.

The scam process remains similar across social media platforms we examined. The accounts post multiple times, often in rapid succession, promising to help fraud victims and sometimes sharing official FBI-released content. Users are then directed to engage with the accounts further through private messages or by visiting domains that emulate the official IC3 website, both of which are designed to collect personal and financial information.

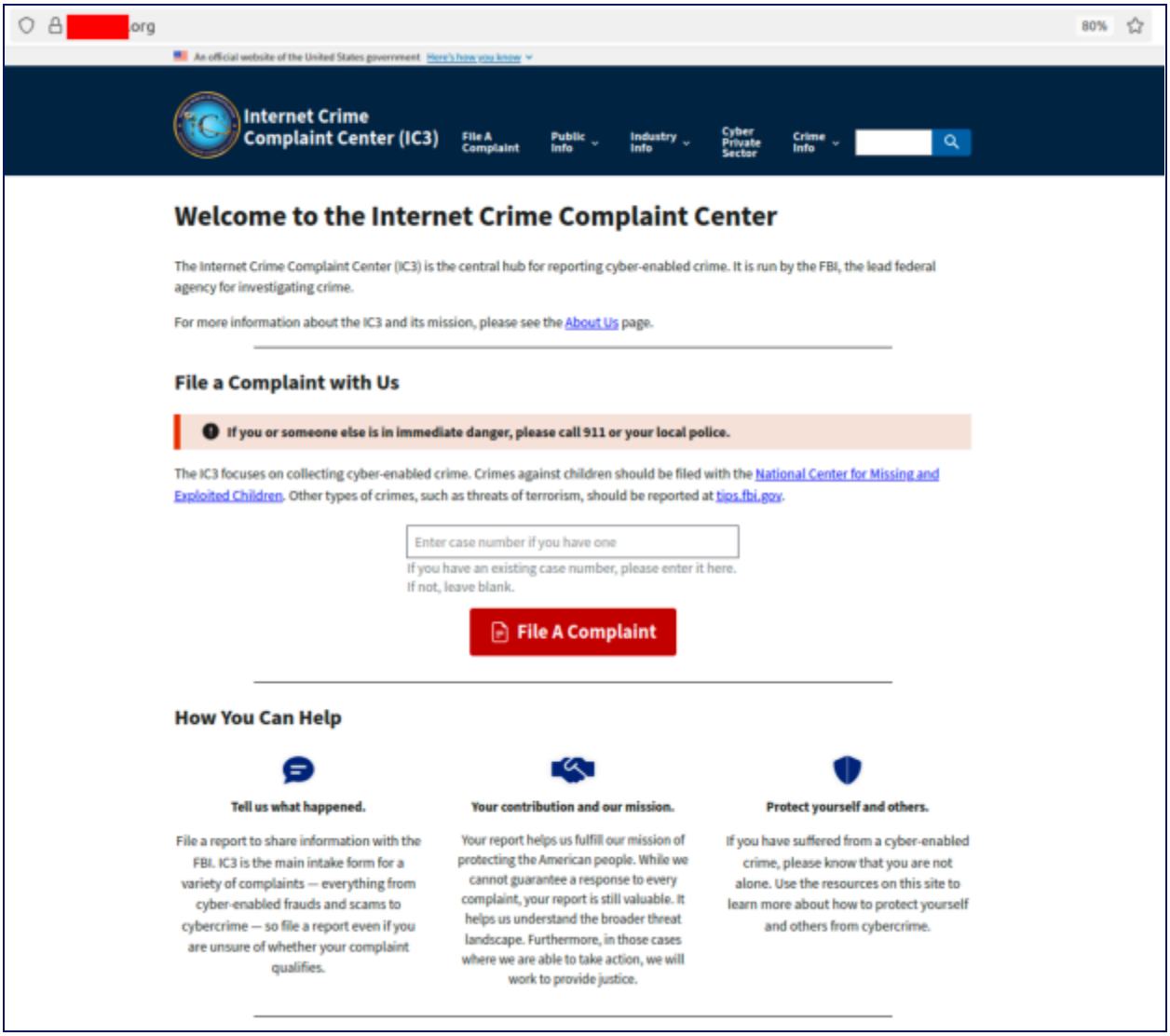
This impersonation extends beyond social media activity. We identified other inauthentic IC3 domains through mainstream search engines, using simple search terms. These sites also mirror the layout and design of the official site, including a “submit complaint” button that requests personal and financial information, which could lead to further exploitation of fraud victims.



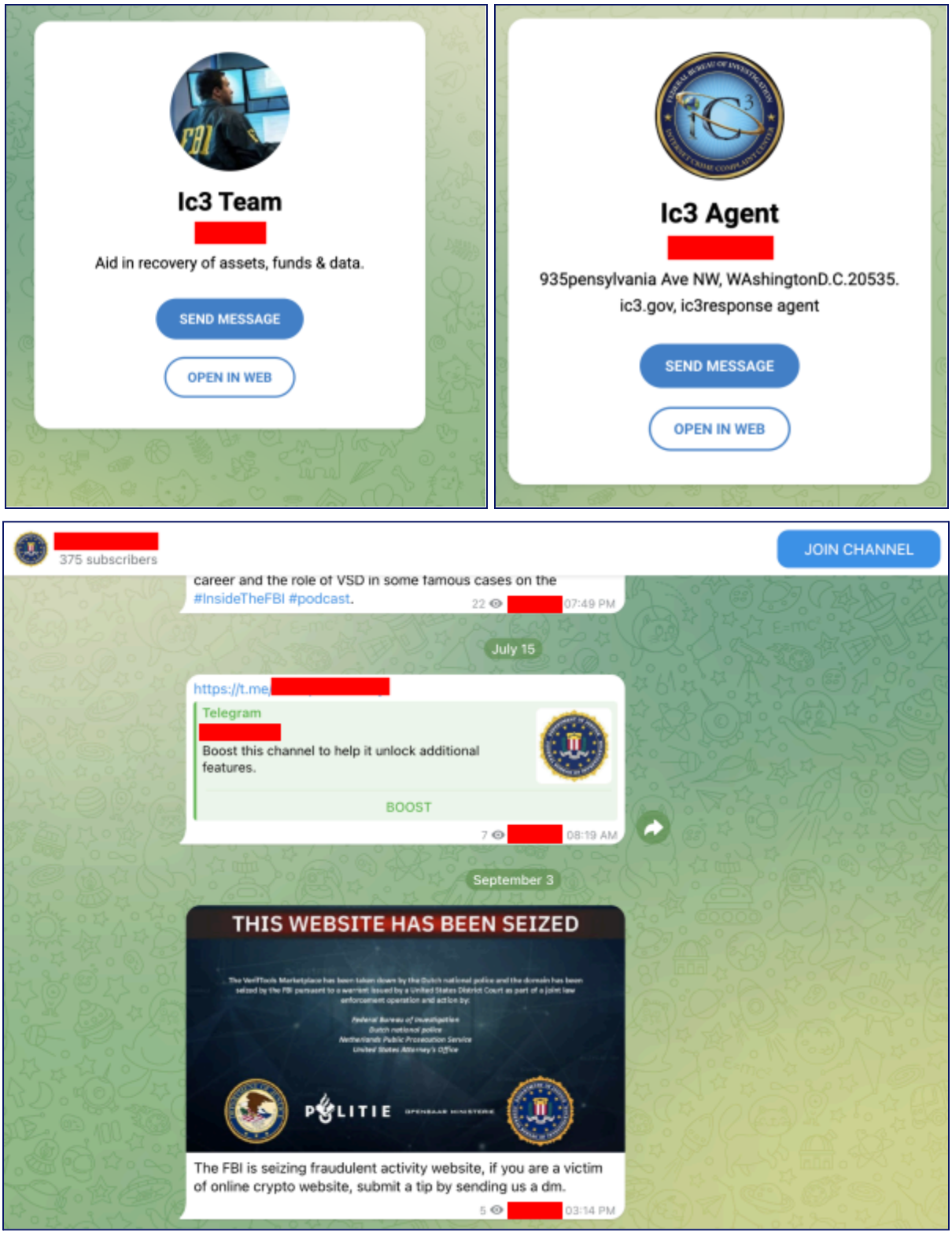
Fraudulent TikTok account impersonating the FBI’s Internet Crime Complaint Center (IC3) with official FBI seals and references to IC3.gov, and encouraging users to visit a website to report scams or recover funds. Redactions added by Graphika.



Ad found in the Meta Ad Library promoting inauthentic IC3 "support" services.



Home page of a fraudulent website that closely mimics the legitimate IC3.gov in banner, layout, and branding. The page invites users to fill out a form to file a complaint, which requires personal and financial information. Redaction added by Graphika.



Telegram channels impersonating the IC3 via official-sounding names, FBI iconography, and case-related language. Redactions added by Graphika.

Estimative Language Legend

Assessments of Likelihood

Graphika uses the following vocabulary to indicate the likelihood of a hypothesis proving correct. If we are unable to assess likelihood due to limited or non-existent information, we may use terms such as "suggest."

Almost No Chance	Very Unlikely	Unlikely	Real Chance	Likely	Very Likely	Almost Certain(ly)
1-5%	5-20%	20-45%	45-55%	55-80%	80-95%	95-99%

Confidence Levels: Indicators of Sourcing and Corroboration

Graphika uses confidence levels to indicate the quality of information, sources, and corroboration underpinning our assessments.

Low Confidence	Medium Confidence	High Confidence
Assessment based on information from a non-trusted source and/or information we have not been able to independently corroborate.	Assessment based on information that we are unable to sufficiently corroborate and/or information open to multiple interpretations.	Assessment based on information from multiple trusted sources that we are able to fully corroborate.

Graphika

About Us

Graphika *is the most trusted provider of actionable open-source intelligence to help organizations stay ahead of emerging online events and make decisions on how to navigate them. Led by prominent innovators and technologists in the field of online discourse analysis, Graphika supports global enterprises and public sector customers across trust & safety, cyber threat intelligence, and strategic communications spanning industries including intelligence, technology, media and entertainment, and global banking. Graphika continually integrates new and emerging technologies into our proprietary intelligence platform and analytic services, empowering our customers with high-precision intelligence and confidence to operate in a complex and continuously evolving information environment.*

For more information or to request a demo, visit our website.