



Stop
Scams
Alliance

A tsunami of cyber-enabled scams: the US must raise its defenses

September 2025

Ken Westbrook

Founder and CEO

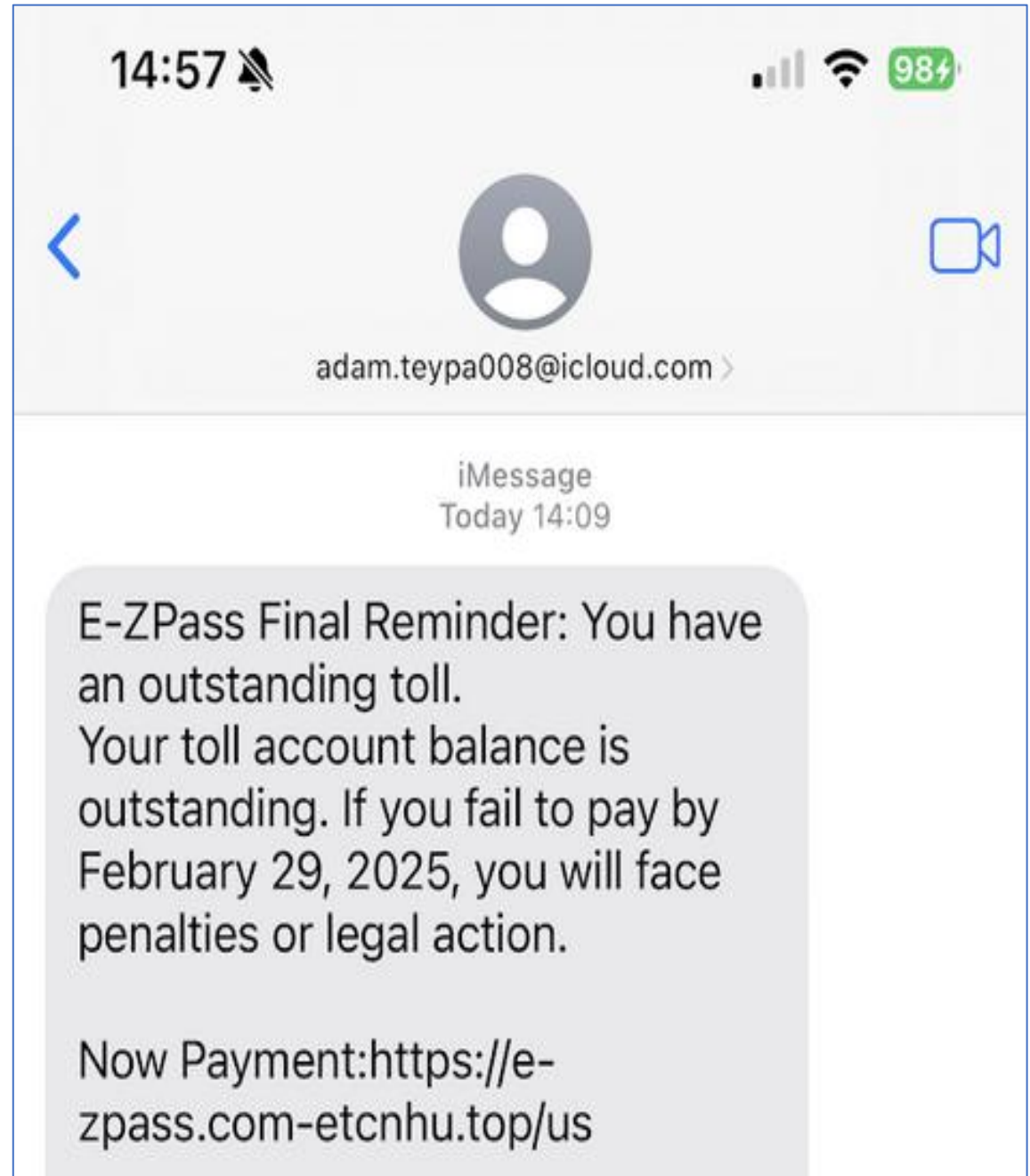
Stop Scams Alliance

The
Economist

*“Cripple the
economies of
the US and
Europe.”*



Who is sending
the toll road
scam via text
messages?



Forbes

FBI Warning As iPhone, Android Users 'Bombarded' By Chinese Attack

A network of Chinese Telegram users is advertising toolkits that allow scammers to easily steal victims' credit card information.



KrebsonSecurity

In-depth security news and investigation



[HOME](#)

[ABOUT THE AUTHOR](#)

[ADVERTISING/SPEAKING](#)

Chinese Innovations Spawn Wave of Toll Phishing Via SMS

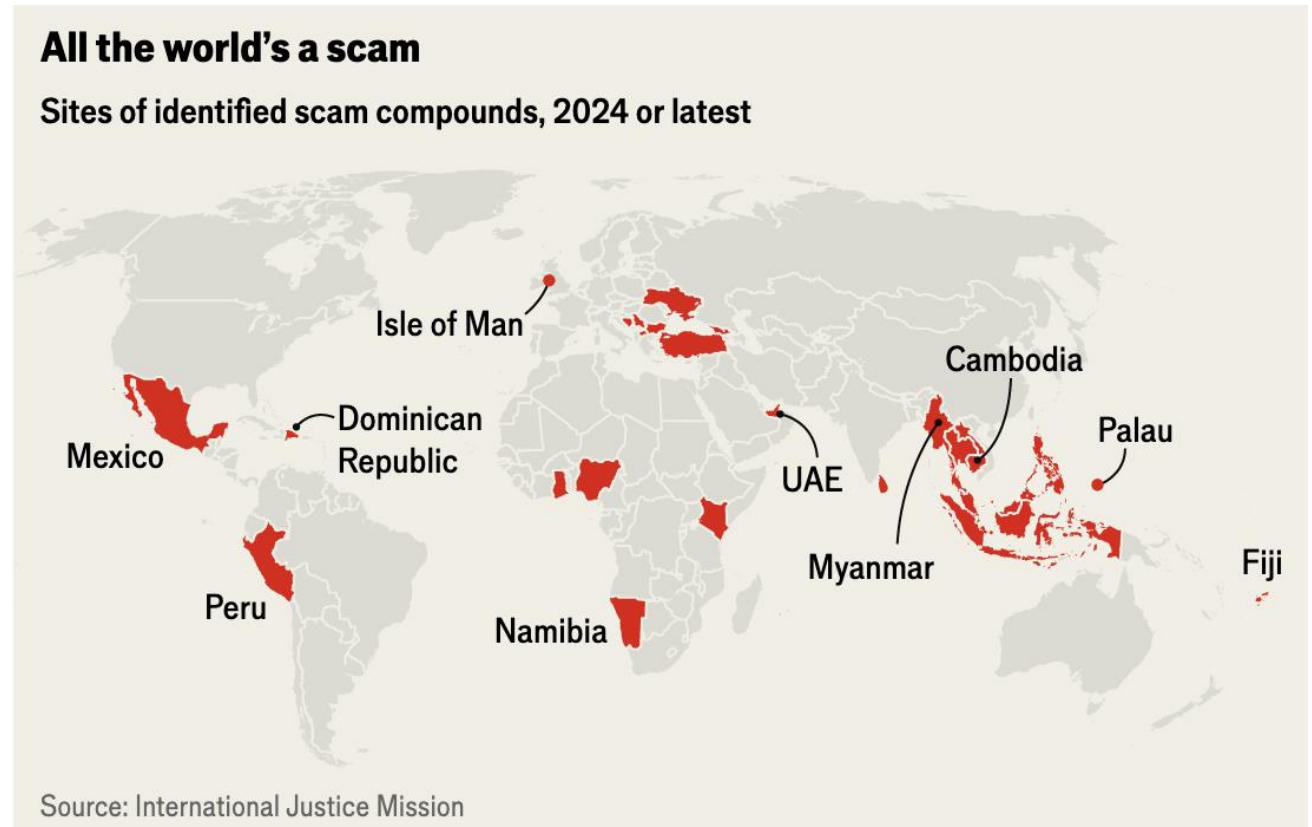
“Multiple China-based cybercriminals are selling distinct SMS-based phishing kits that each have hundreds or thousands of customers.

Cyber Scamming Goes Global: Sourcing Forced Labor for Fraud Factories

“Though media coverage often focuses on Southeast Asia, scam centers have also been discovered as far away as [Ghana](#), [Peru](#), the [UAE](#), and [Mexico](#). Many, though not all, of these centers can trace their ownership back to Chinese-speaking criminal groups.”

Where are the perpetrators?

FBI: “[Cryptocurrency investment fraud](#), also known as "pig butchering," originated in Southeast Asia and are being perpetrated by organized crime groups operating from scam compounds in **Southeast Asia, the Middle East, Africa, and South America.**”



Most scam compounds run by ethnic Chinese crime bosses

<https://www.fbi.gov/how-we-can-help-you/victim-services/national-crimes-and-victim-resources/operation-level-up>

Where are the perpetrators?

India. Call center and tech support scams “primarily emanate from call centers in South Asia, mainly India,” according to the [FBI](#).

Nigeria and Ivory Coast: The Nigerian Black Axe crime syndicate and similar groups are responsible for most of the world’s cyber-enabled financial fraud, according to [Interpol](#). West Africa is a “potential emerging hub region.”

- “Sextortion” scams that target teens are “usually located in **Nigeria, Ivory Coast** or the **Philippines**,” according to the [FBI](#).

Mexico: “TCOs such as the Jalisco New Generation Cartel (CJNG) are increasingly targeting U.S. owners of timeshares in Mexico through [scams],” according to the [US Treasury Department](#). Proceeds used for “manufacturing and trafficking of illicit fentanyl and other synthetic drugs into the United States.”

PRESS RELEASES

Treasury Targets Terrorism and Timeshare Fraud in Mexico



August 13, 2025

Scams Targeting U.S. Victims Produce Significant Revenue for CJNG

Sanctioning Cartel de Jalisco Nueva Generación Leaders Operating Timeshare Fraud Schemes

PRESS STATEMENT

TAMMY BRUCE, DEPARTMENT SPOKESPERSON

AUGUST 13, 2025

Where are the perpetrators



UK government estimates 70 percent of scams originate overseas

“The volume of fraud, its capacity to undermine public confidence in the rule of law, and its potential negative effect on the UK’s financial reputation, means it should be considered a **national security threat.**”

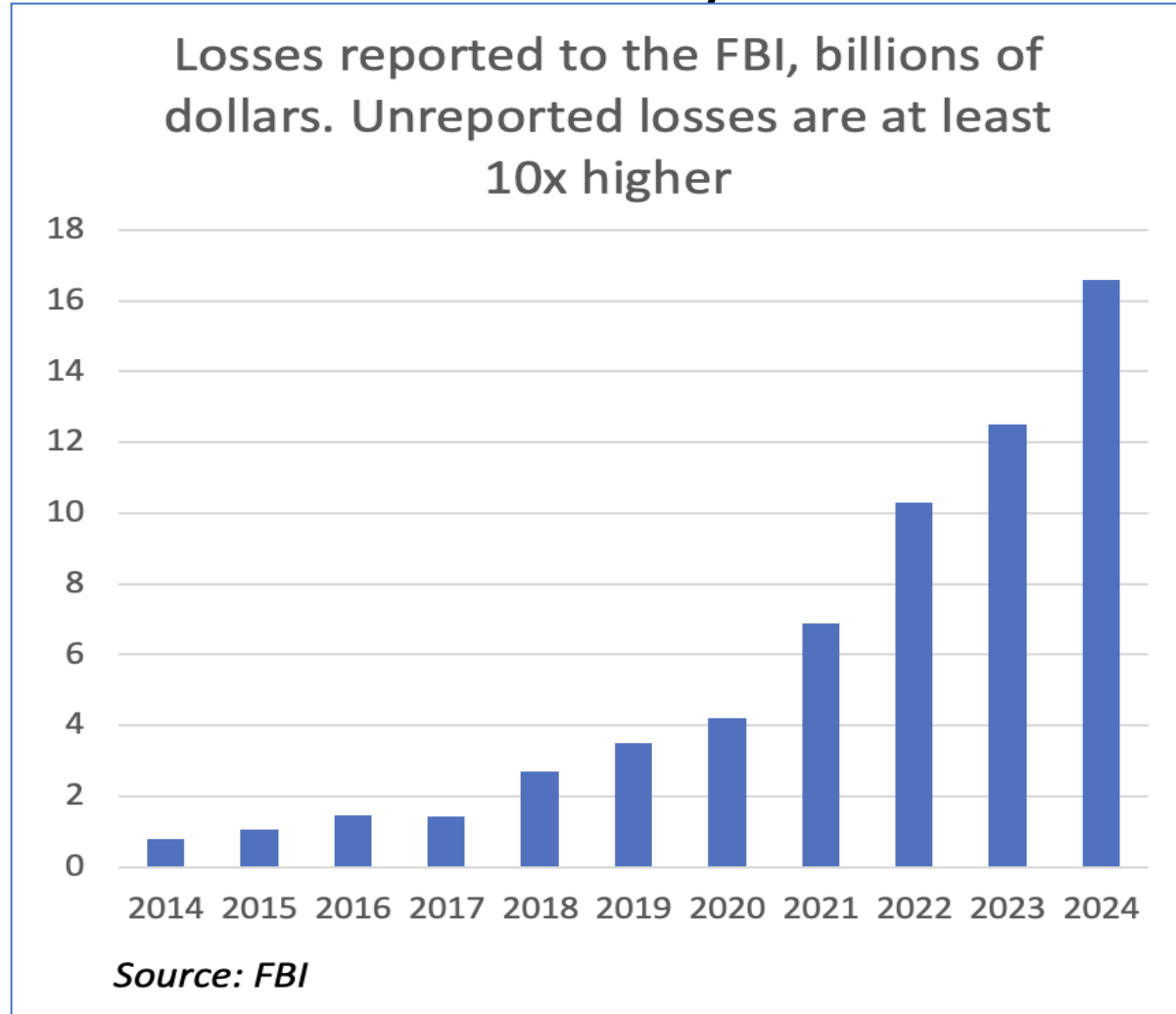
US has no official estimate. Unofficially: 90 percent?

Grassley Opens Judiciary Hearing on Threats Posed by Scammers and Transnational Crime Networks.

- “Transnational organized crime groups are targeting all of us with industrial-scale fraud.”
- “Transnational crime networks are using American dollars for drug trafficking, human trafficking, arms trafficking and other evil projects.”
- “Let me be absolutely clear: this is a national security crisis hiding in plain sight. And we’re inadvertently funding it.”

20-fold increase in reported fraud losses since 2014

US Secret Service: “Transnational fraud threats far exceed the capacity of US law enforcement to sufficiently deter”*



US LE officials in 9/2024
Congressional hearings:

- “Epidemic”
- “Tsunami”
- “critical national security concern”

**September 18, 2024 hearing before the House Financial Services Committee*

Annual US Consumer Scam Victims and Losses

	Reports	Total (includes under reported)
Annual victims	987,520 (FTC) 859,532 (FBI)	21 million (Gallup)
Annual losses	\$12.5 billion (FTC) \$16.6 billion (FBI)	\$158.3 billion (FTC)

57,000 scammed each day in the US



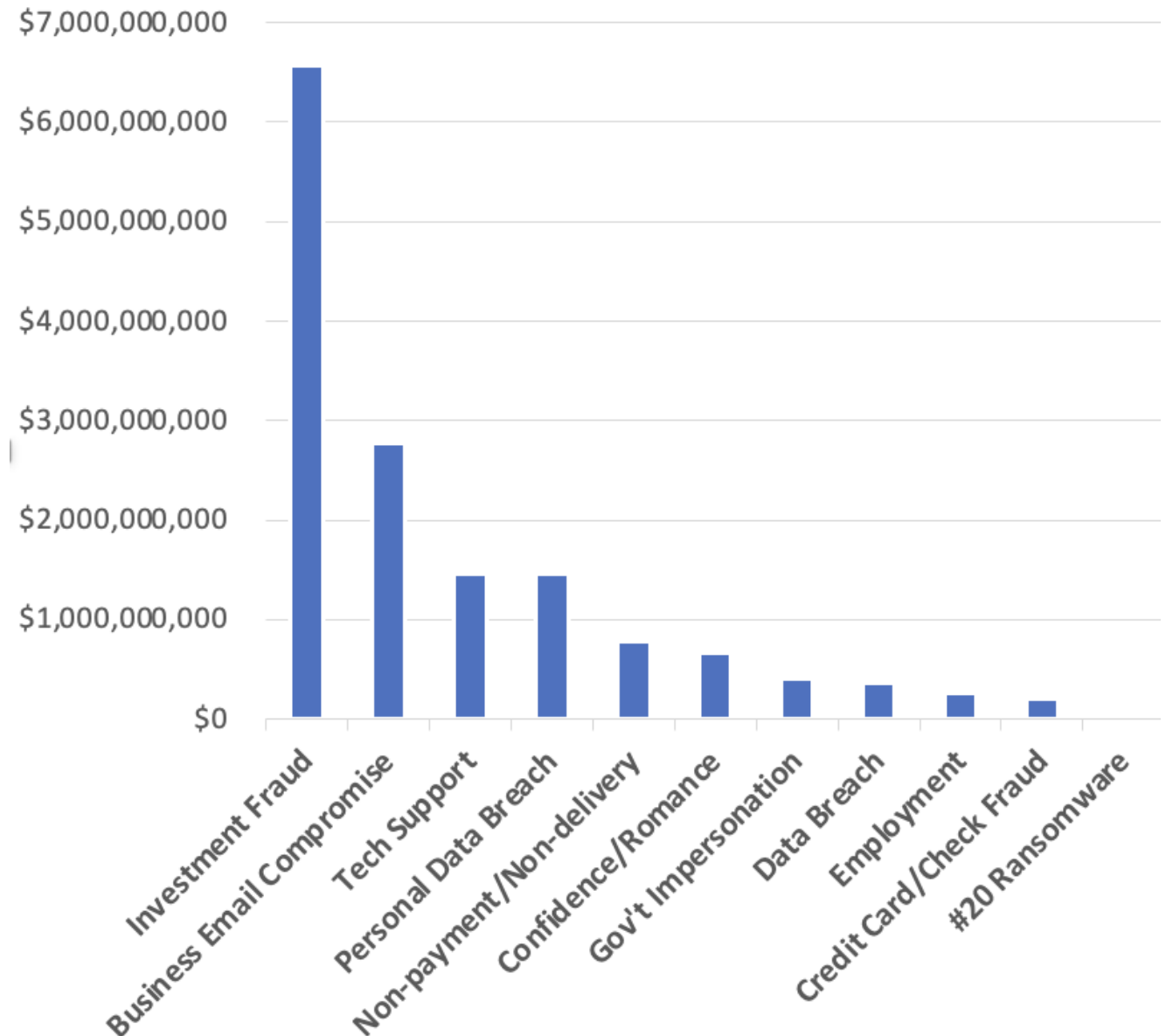
Costliest Scams

Top scams:

- Investment
- Business Email Compromise
- Tech Support
- Personal Data Breach

(above four account for 74% of reported scam losses)

What are the top ten costliest scams?
Losses reported to the FBI in 2024



Impersonation scams

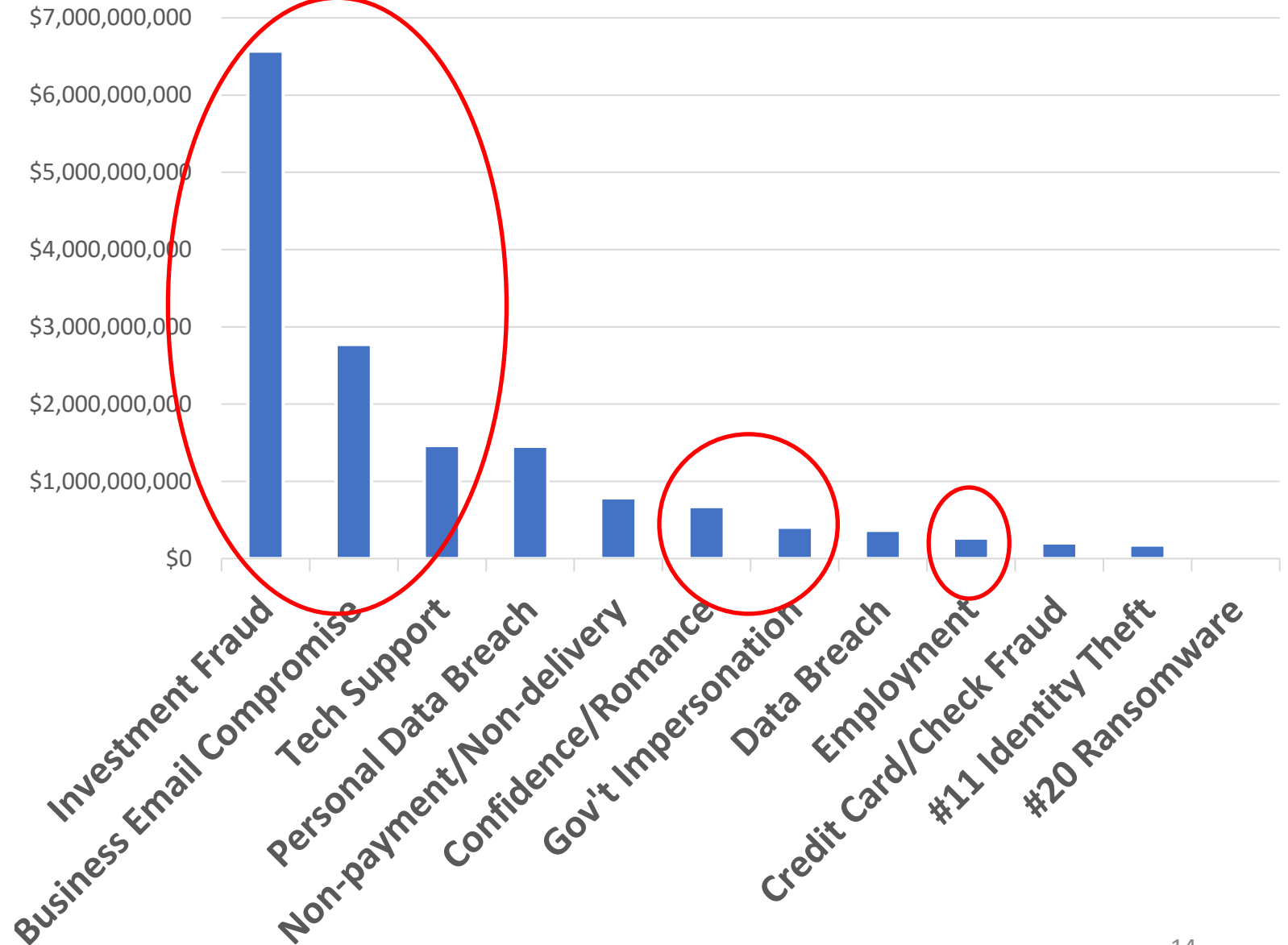
responsible for
3/4 of losses



FEDERAL TRADE COMMISSION
PROTECTING AMERICA'S CONSUMERS

“Scams that impersonate well-known businesses and government agencies are consistently among the top frauds”

Losses reported to the FBI in 2024



7 August 2025

For Release



FEDERAL TRADE COMMISSION
PROTECTING AMERICA'S CONSUMERS

FTC Data Show a More Than Four-Fold Increase in Reports of Impersonation Scammers Stealing Tens and Even Hundreds of Thousands from Older Adults

In 2024, adults 60 and over reported losing millions to scammers pretending to be from trusted government agencies, businesses

The antidote for impersonation is authentication!

What does the future hold?

- Artificial intelligence
- Increasing use of fast payments, cryptocurrency
- The UK and Australia are raising their defenses

Criminals are shifting to target the US

Secret Service testimony on 18 September 2024: “as ... other jurisdictions implement new customer identification and authentication restrictions related to financial accounts, [criminals] are shifting their activity to target US citizens and financial institutions”

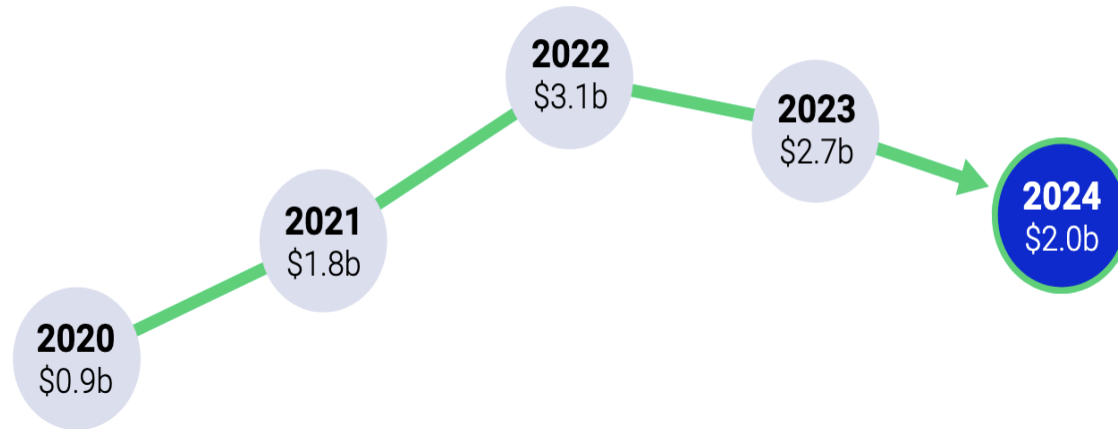
It is possible to bend the curve!

Australia: Reported losses down 35% since 2022

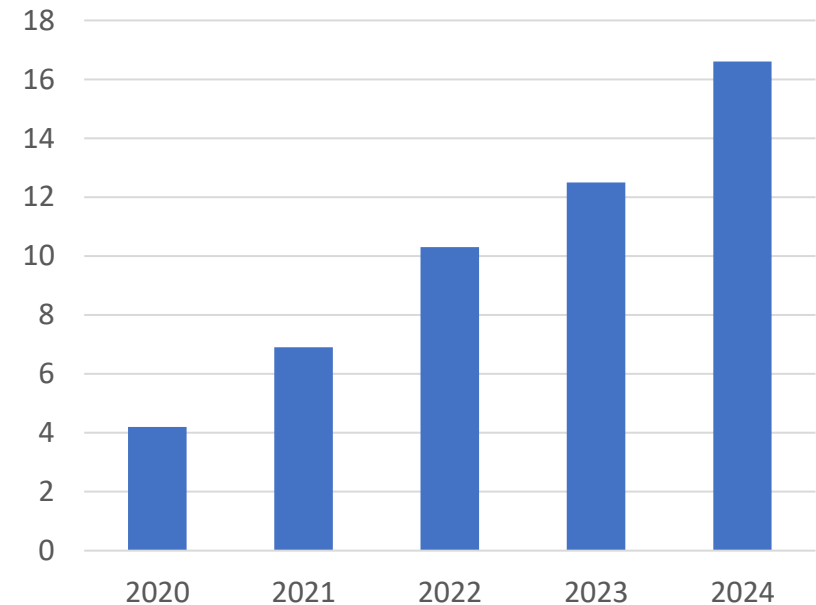
US: Reported losses up 61% since 2022



Combined losses over last 5 years



Losses reported to the FBI



UK: Reported losses down 11% since 2021

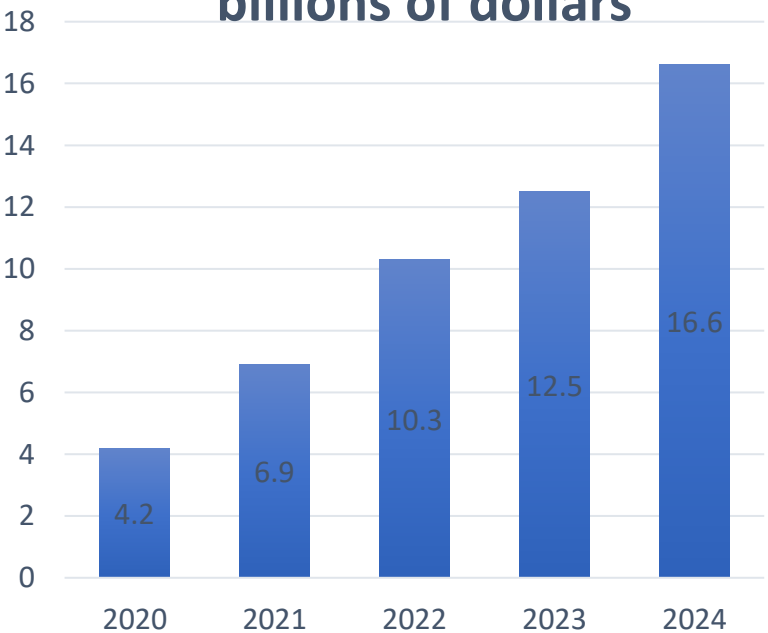
US: Reported losses up 141% since 2021



Total fraud cases and losses, millions



Losses reported to FBI/IC3, billions of dollars



Source: UK Finance <https://www.ukfinance.org.uk/system/files/2025-05/UK%20Finance%20Annual%20Fraud%20report%202025.pdf>

Step 1: Priority, strategy, someone in charge



In 2022, the Australian government made fighting scams a national priority

- Scam czar: Assistant Treasurer and Minister for Financial Services

“We will make Australia one of the hardest targets in the world for scammers”



May 2023: UK published *“Fraud Strategy: Stopping Scams and Protecting the Public”*

- Fraud Minister: Lord David Hanson, Home Office (former MP)

UK’s goal: “to make the UK the safest place in the world to be online”

Step 2: Centralized data collection and fusion

Australia established a National Anti-Scam Centre in 2023 to centralize data collection

- Banks, telecom companies, internet service providers, social media companies, regulators, and law enforcement can share information on scams, enabling faster action and greater protection

Ten countries have data fusion hubs

- | | |
|-----------------------|-------------------------|
| • Singapore (2019) | • Thailand (2023) |
| • Malaysia (2022) | • Australia (July 2023) |
| • Saudi Arabia (2022) | • India (2024) |
| • South Korea (2023) | • Indonesia (2024) |
| • Taiwan (2023) | • Maldives (2025) |

Australia combats scams through data fusion

Partnership: law enforcement,
regulators, consumer groups,
banks, telcos, social media

Three key functions:
-- Collaboration (technology
and intelligence sharing)
-- Disruption
-- Awareness and protection


Future state: National Anti-Scam Centre regular data sharing



Step 3: Disrupt the scam business model by preventing criminals from abusing the internet, messaging, and payment systems

Tools: authentication, block lists, allow lists to address

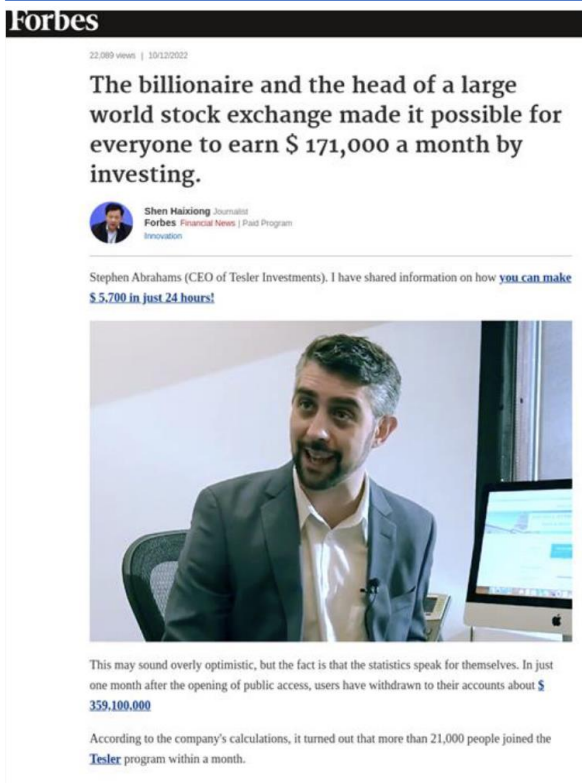
- Fraudulent and malicious online ads
- Malicious websites
- Fake investment websites
- Spoofed phone calls
- Spoofed text messages



Authentication
makes it harder
for criminals to
hide!

Authentication of financial advertising

Example of fake financial ad



Google: requires financial services advertisers to be on a government authorized list in 17 countries:

- UK, Australia, Brazil, France, Germany, India, Indonesia, Ireland, Italy, New Zealand, Portugal, Singapore, South Korea, Spain, Taiwan, Thailand, and Turkey
- Result: "pronounced decline in reports of ads promoting financial scams"

Meta: Since 2024 in the **UK**, financial ads must be authorized by the UK's Financial Conduct Authority

- Policy extended to **Taiwan** in Aug 2024; **Australia** and **India** in 2025

Australia: Apple, Discord, Google, Meta, Snap, TikTok, Twitch, X and Yahoo) signed a voluntary industry code in 2024 that requires moving toward "reasonable measures to confirm that an advertiser holds the necessary financial services license"

<https://blog.google/technology/ads/expanding-our-efforts-to-combat-financial-fraud-in-ads/>

<https://www.facebook.com/business/help/719892839342050>

Australian business community supports authentication of text messages

Australia's SMS Registry has received broad support from consumer groups, financial institutions, telecommunications providers, and government agencies (89% of industry feedback supported mandatory model)



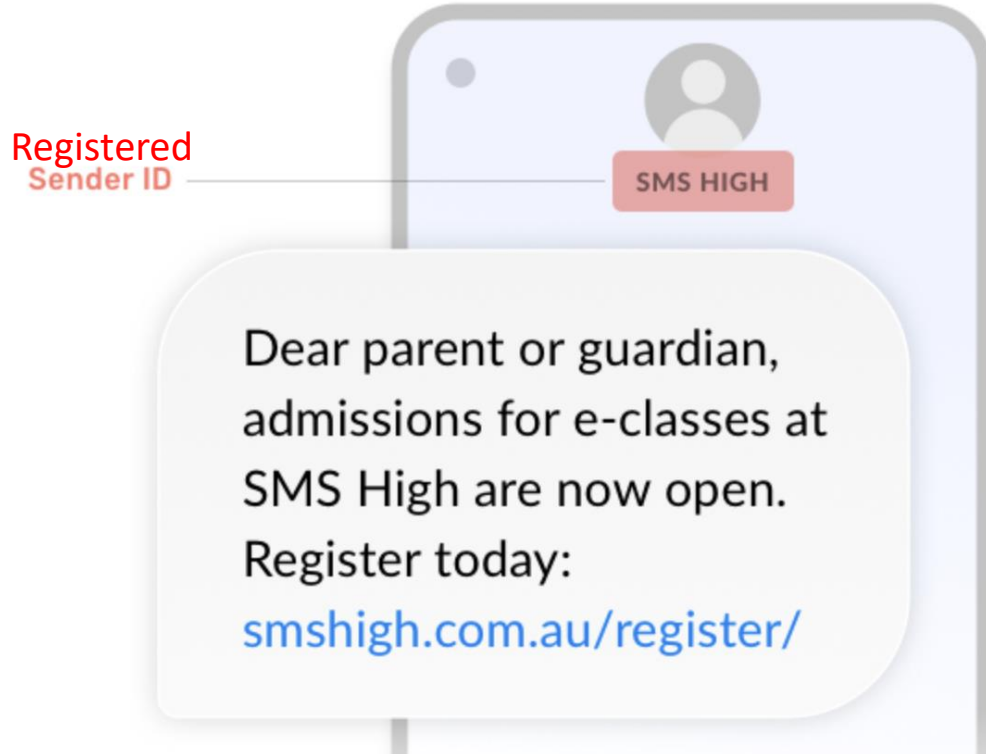
TPG Telecom: only by “developing a mandatory, trusted, closed ecosystem for sending alphanumeric Sender ID SMSs will the public, businesses, and the telecommunication industry see a reduction in scam communications.”



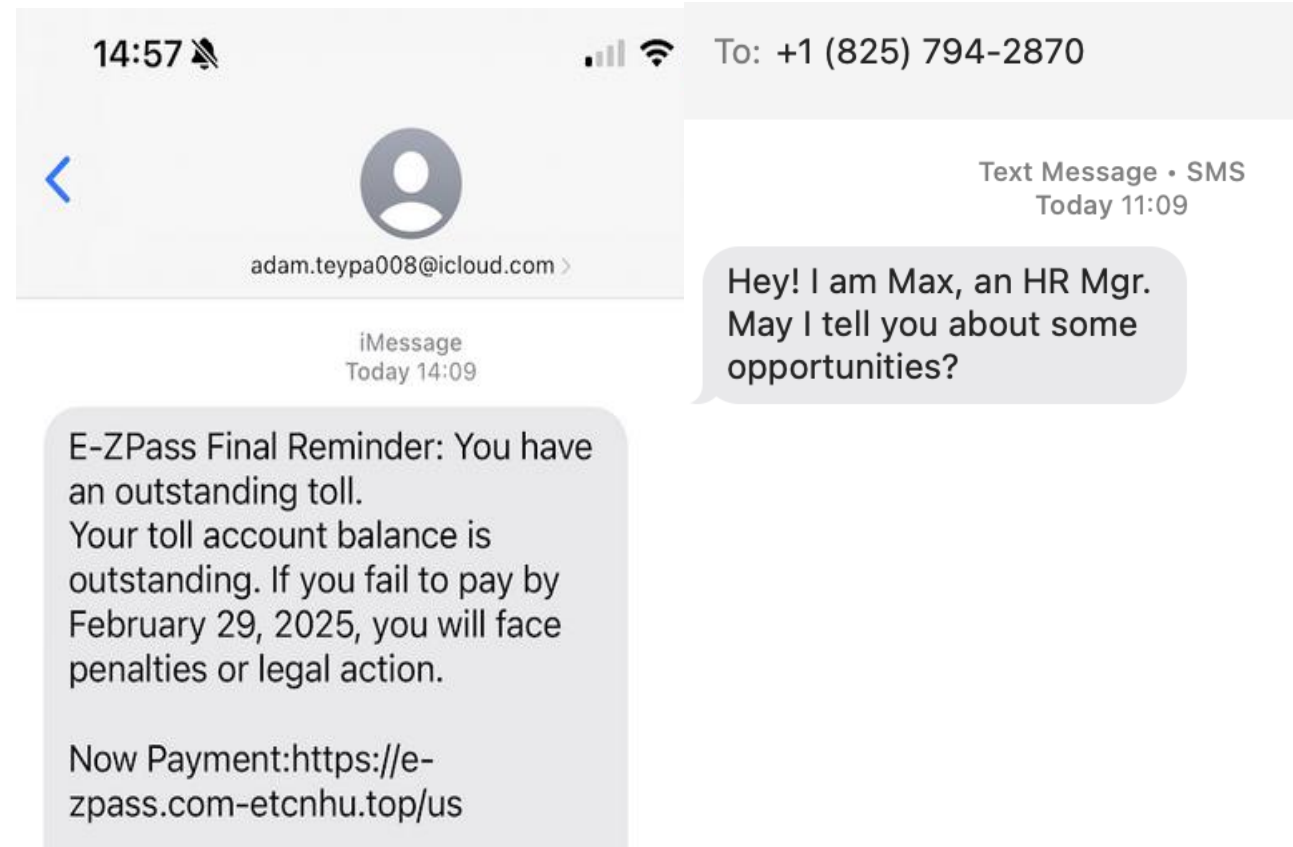
“The ABA welcomes further progress by the Federal Government to establish a mandatory SMS Sender ID register with an enforceable industry standard, in what will be a critical preventative measure in the fight against scammers.”

Authenticated text messages available in UK, Australia, Ireland, Spain, Singapore

Australia: Authenticated



US: Not authenticated



Australia implementing authentication of text messages as of 15 December 2025

(Senders of text messages must be registered)

	SENDER HAS NOT REGISTERED THE SENDER ID	SENDER HAS REGISTERED THE SENDER ID
SENT VIA NON-REGISTERED CARRIER OR CSP	Intended recipient will not receive the message (message is effectively blocked)	Intended recipient will not receive the message (message is effectively blocked)
SENT VIA REGISTERED CARRIER OR CSP	Message will be delivered with over-stamped sender ID reading 'Likely SCAM'	Message will be delivered with sender ID

Does not apply to texts sent from personal devices. See: <https://www.acma.gov.au/sms-sender-id-register>

Blocking foreign phone calls that display a domestic CLI

22 countries block inbound international calls that spoof domestic phone numbers: UK, Australia, Sweden, Finland, Norway, Denmark, Belgium, Latvia, Lithuania, Malta, Romania, Oman, Saudi Arabia, UAE, Bahrain, India, Singapore, Spain, Czech Republic, Ireland, Poland, Italy

UK: One of the companies involved saw a 65-percent reduction in complaints about scam calls

Australia: scam call complaints fell by 72 percent as a result of similarly aggressive call blocking

Call volume dropped by 90 percent in India , 70 percent in Taiwan, and 60 percent in Finland

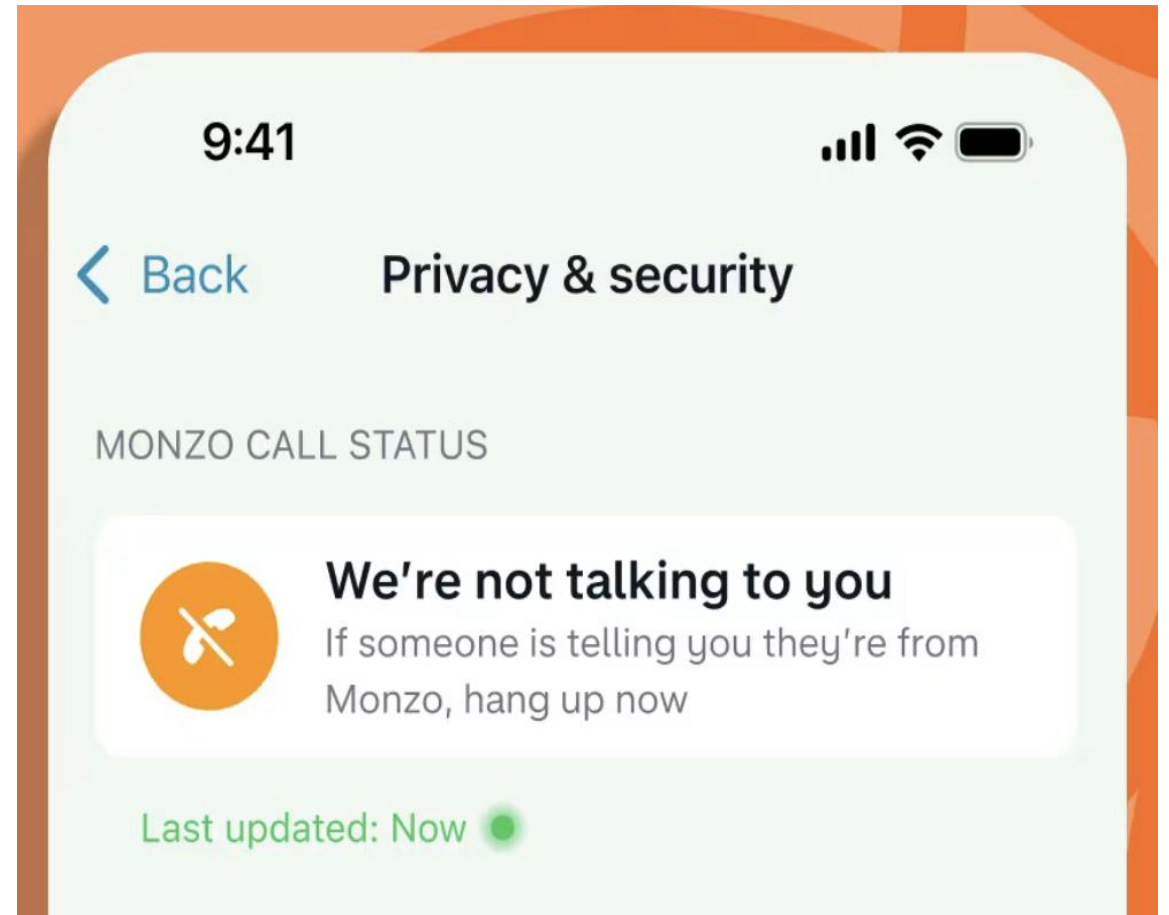
“159”

Dedicated, easy-to-remember telephone number that allows UK consumers to connect safely and directly to their bank's fraud department

--More than one million calls have been made to 159 since inception.

--Participants: Major banks like Barclays, HSBC, Lloyds, Nationwide, Monzo, NatWest, Santander, Starling, TSB, Virgin Money, etc.

In-App Authentication



Australia: National-level identification and takedown of fraudulent investment websites



MEDIA RELEASE (25-026MR)

ASIC shuts down 130 investment scam websites per week

Published 28 February 2025


Since July 2023, ASIC has coordinated the removal of more than more than 10,000 investment scam websites and online advertisements

Investment scam losses decreased by 35 percent from 2023 to 2024

<https://asic.gov.au/about-asic/news-centre/find-a-media-release/2024-releases/24-180mr-online-investment-trading-scams-top-asic-s-website-takedown-action/>

<https://ministers.treasury.gov.au/ministers/stephen-jones-2022/media-releases/new-data-shows-scam-losses-continue-fall-under-labor>

National-level identification and takedown/blocking of fraudulent websites

- Most website takedowns done by  an arm of GCHQ
- UK organizations and citizens send 20,000 reports a day of suspicious emails and URLs – one every 5 seconds!
- Malicious URLs removed in less than 6 hours on average
- 235,000 malicious URLs removed since April 2020

New “Share and Defend” program works with internet service providers (ISPs) and other tech companies to block access to malicious websites

- Participants include: **BT, Vodafone, Talk Talk**

UK: Taking Down Cryptocurrency Scams

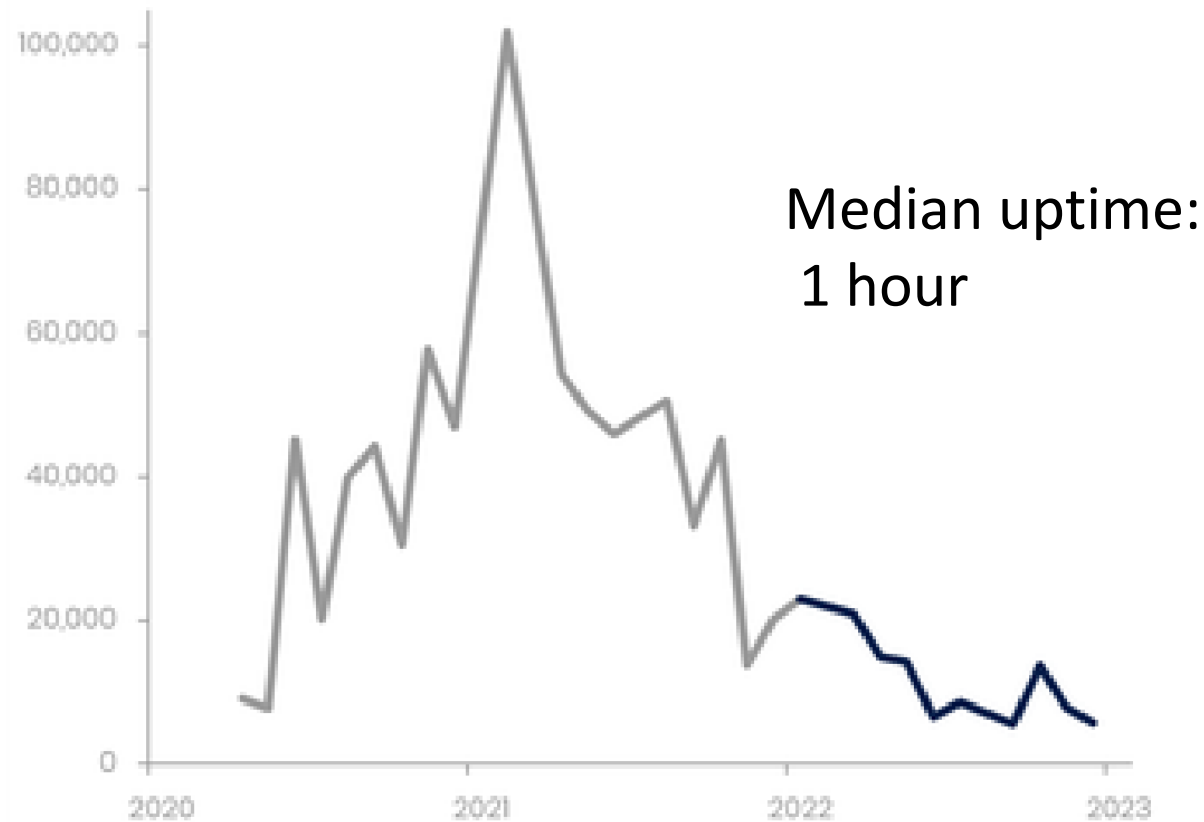
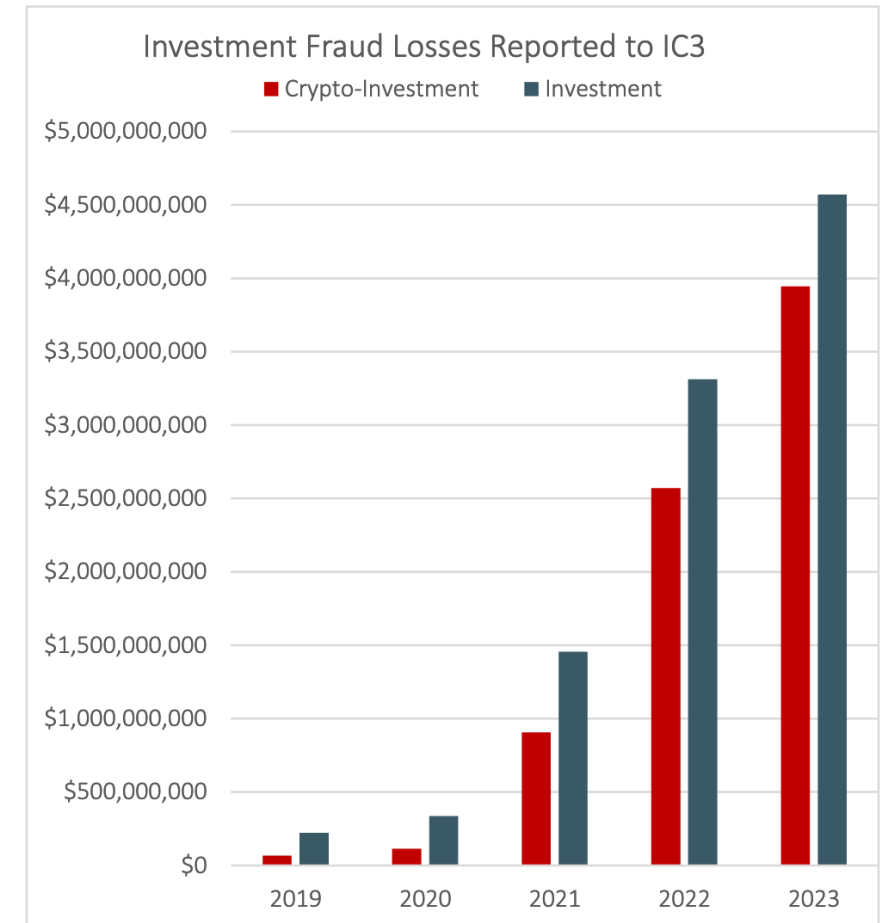


Figure 1: Number of takedowns against cryptocurrency investment scams

<https://www.ncsc.gov.uk/files/ACD6-full-report.pdf>

US: Crypto Scam Losses Increased 53% Between 2022 and 2023



Anti-Fraud Initiatives	UK	Australia	US
Comprehensive national strategy	✓	✓	
Someone in charge	✓	✓	
Annual government survey measures fraud	✓	✓	
Nationwide public education	✓	✓	
Centralized fraud reporting	✓	✓	
Phone: Block inbound international calls that spoof domestic numbers	✓	✓	
Texts: Authenticated sender ID	✓ private	✓ government	
Fraudulent websites: national takedown	✓	✓	
Public-private partnership	✓	✓	
Boost law enforcement resources	✓ adding 400 investigators	✓	
Boost government investment	£400m (\$500m)	180m AUD (\$115m)	

Summary

- The US is under attack by transnational organized crime
- Criminal use of AI will add fuel to the fire
- Main avenues of attack:
 - Fraudulent and malicious ads
 - Malicious websites
 - Fake investment websites
 - **Voice calls**
 - **Text messages**
- Other countries are seeing success by adding authentication methods and data fusion centers
- Criminals are telling Secret Service informants that they see the US as the softest target because our authentication practices are weaker
- **The US must raise its defenses**

What can people in this
room do?





Stop Scams Alliance

A 501(c)(3) nonprofit whose mission is to significantly reduce scams in the United States through a comprehensive, systemic approach involving public-private partnership and cross-sector cooperation from technology, telecom, financial institutions, consumer advocacy groups, and government.

- The focus is to stop scams at the source, before they reach the consumer in the first place.

www.StopScamsAlliance.org

ken@StopScamsAlliance.org

<https://www.linkedin.com/in/kennethwestbrook/>