

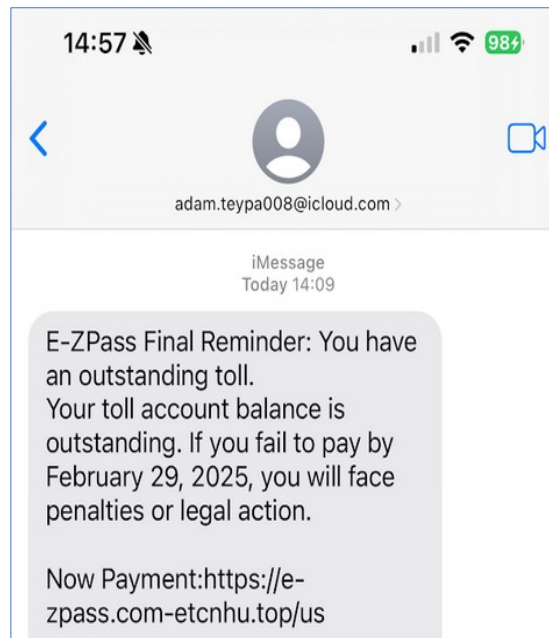


Cyber-enabled scams: the US must raise its defenses

May 2025

Ken Westbrook
Founder and CEO
Stop Scams Alliance

Who is sending
the toll road
scam 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.

Instead of using standard SMS, which can be filtered by telecom operators, these groups send phishing messages via iMessage (for Apple users) and RCS (for Android users). This approach bypasses network-level anti-spam protections, relying instead on device-level filters from Apple and Google



Using AI to stop tech support scams in Chrome
May 8, 2025

...in the future we plan to use [the on-device Gemini Nano large language model (LLM)] to help detect other popular scam types, such as package tracking scams and unpaid toll scams

The
Economist

Leaders | International crime

The vast and sophisticated global enterprise that is Scam Inc

Online fraud leaves nobody safe



The
Economist

*"Cripple the
economies of
the US and
Europe."*



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**.”

All the world's a scam

Sites of identified scam compounds, 2024 or latest



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? (2)

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](#).

- “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.”

Where are the perpetrators (3)



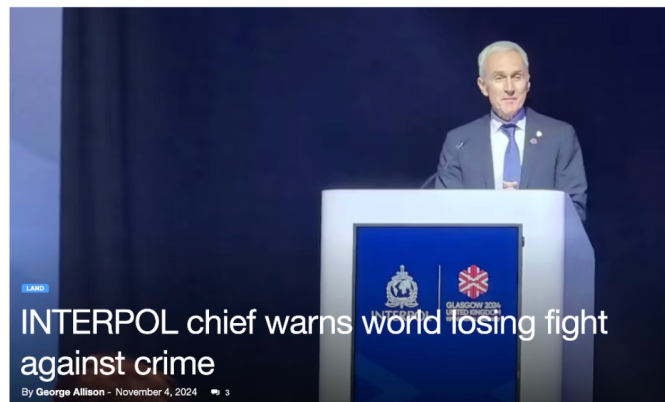
UK government estimates 70 percent of scams originate overseas

“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?

INTERPOL Chief Stock:

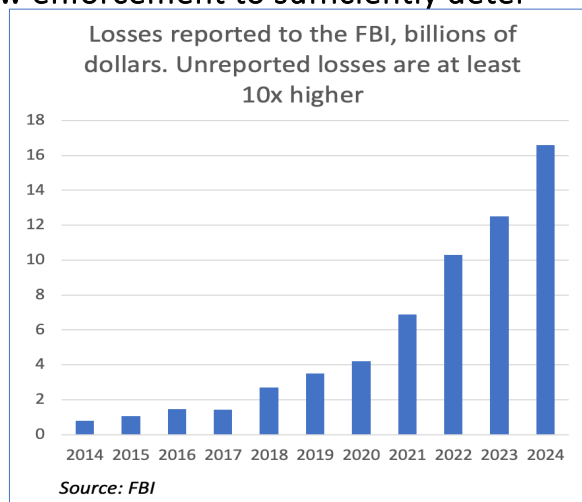
"I finish my mandate with significant concerns about the ability of global law enforcement to keep the world safe"



"We face an adversary with relentless ambition. An adversary able to turn to new tools like AI to supercharge their frauds and cyber enabled crimes. We are in the fight of our lives. For our communities, and for our global security. Nothing else matters."

21-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

US Consumer Scam Victims and Losses

	Reports
Annual victims	987,520 (FTC) 859,532 (FBI)
Annual losses	\$12.5 billion (FTC) \$16.6 billion (FBI)

US Consumer Scam Victims and Losses

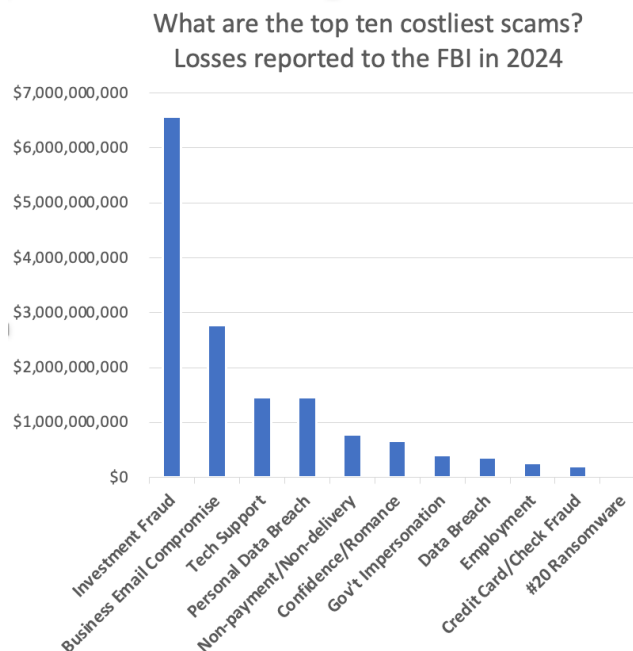
	Reports	Total (includes under reported)
Annual victims	987,520 (FTC) 859,532 (FBI)	21 million (Gallup)
Annual losses	\$12.5 billion (FTC) \$16.6 billion (FBI)	\$158.3 billion (FTC)

Costliest Scams

Top scams:

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

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



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

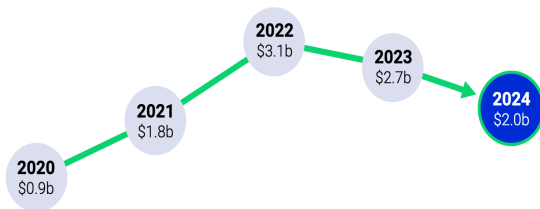
Secret Service testimony on 18 September 2024: “as ... other jurisdictions implement new customer identification and authentication restrictions related to financial accounts, [criminals] are shifting their activity to target US citizens and financial institutions”

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



<https://www.accc.gov.au/system/files/targeting-scams-report-2024.pdf>



Losses reported to the FBI

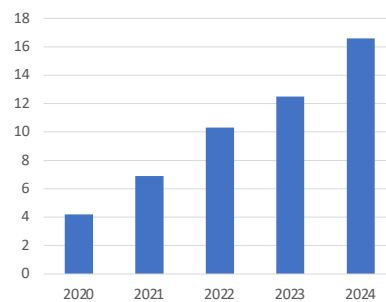




Chart 1 Total fraud losses and case volumes, millions

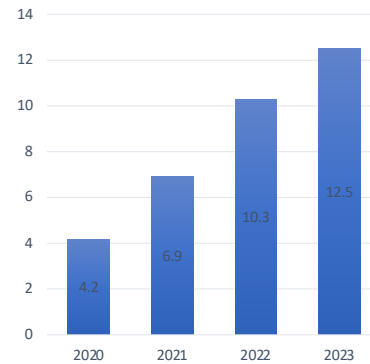


<https://www.ukfinance.org.uk/system/files/2024-06/UK%20Finance%20Annual%20Fraud%20report%202024.pdf>

Source: UK Finance



Losses reported to FBI/IC3, billions of dollars



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

Nine countries have data fusion hubs

- Singapore (2019)
- Malaysia (2022)
- Saudi Arabia (2022)
- South Korea (2023)
- Hong Kong
- Taiwan (2023)
- Thailand (2023)
- Australia (July 2023)
- India (2024)



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

<https://www.accc.gov.au/system/files/NASC-Quarterly-update-Q3-2024.pdf>

Future state: National Anti-Scam Centre regular data sharing



The US needs centralized reporting for fraud!

Centralized reporting would help law enforcement and victims



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 ads
- Malicious URLs
- Fake investment websites
- Spoofed phone calls
- Spoofed text messages

Authentication makes it harder for criminals to hide!

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



ASIC
Australian Securities
Investments Commis

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  National Cyber Security Centre 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**

<https://www.ncsc.gov.uk/news/british-business-support-crucial-in-removing-scams>

25

UK: Taking Down Cryptocurrency Scams

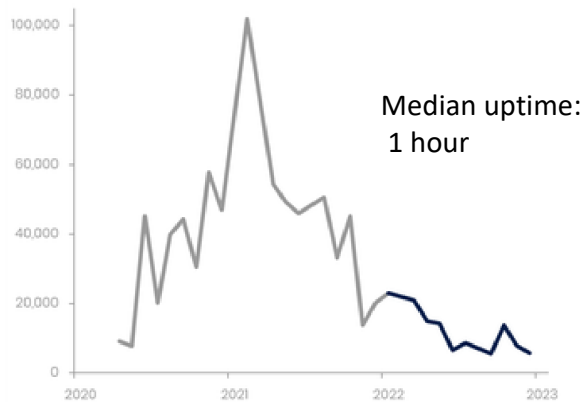
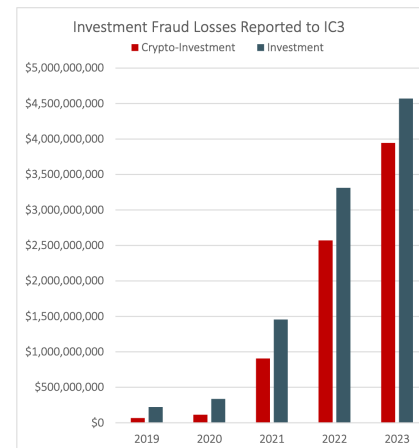


Figure 1: Number of takedowns against cryptocurrency investment scams
<https://www.ncsc.gov.uk/files/ACD6-full-report.pdf>

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



Blocking foreign phone calls that are spoofed

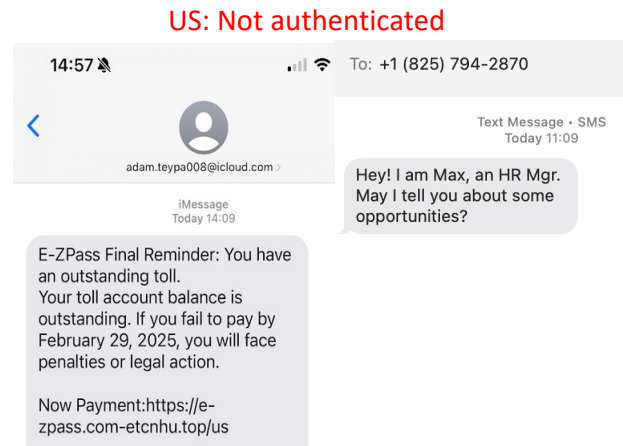
19 countries block inbound international calls that spoof domestic phone numbers: UK, Australia, Sweden, Finland, Norway, Germany, Belgium, Latvia, Lithuania, Oman, Saudi Arabia, India, Singapore, Taiwan, Spain, Czech Republic, Ireland, Poland, Malta

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

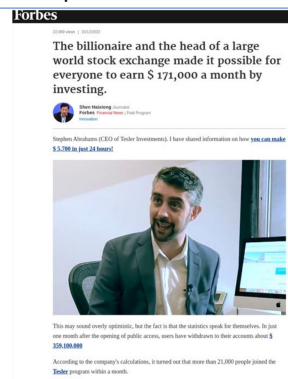
Call volume dropped by 90 percent in India , 70 percent in Taiwan, and 60 percent in Finland

Authenticated text messages available in UK, Australia, Singapore



Using white list to authenticate financial advertising

Example of fake financial ad



Google: Since 2021 in the **UK**, Google requires financial advertisers to be on a government authorized list

- Result: “pronounced decline in reports of ads promoting financial scams”
- In 2022, Google expanded its verification policy to **Australia, Singapore, and Taiwan**

Meta: Since 2024 in the **UK**, financial ads must be authorized by the UK's Financial Conduct Authority before the ad is permitted on Meta's platforms

- Policy extended to **Taiwan** as of 1 Aug 2024;
- **Australia** in February 2025

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

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

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. spoofing	✓ private	✓ government	
Fraudulent websites: national takedown	✓	✓	
Public-private partnership	✓	✓	
Boost law enforcement resources	✓ adding 400 investigators	✓	
Boost government investment	£400m (\$500m)	180m AUD (\$115m)	

The US needs a national, whole-of-government strategy, with goals, metrics, resources



- White House led
- Cross government (Treasury, FBI, DHS/CISA, USSS, FTC, FCC, SEC, CFTC, CFPB, etc.)
- Cross industry (tech, telecom, financial, consumer groups)
- Public/private partnership

FOCUS: Stopping scams at the source through centralized data fusion
Bolster education and law enforcement



Stop
Scams
Alliance

Initiatives

Data collection. Good public policy requires good data

- Gallup survey

Strategy

- Office of National Cyber Director

Awareness

- Op-eds



The Washington Post



THE CIPHER BRIEF

- Presentations



Stop
Scams
Alliance

Our strategy initiative



JANUARY 13, 2025

We Must Protect Americans Against Cyber-Enabled Fraud



ONCD > BRIEFING ROOM > BLOG

January 13, 2025

By National Cyber Director Harry Coker, Jr.

“The Federal government needs to lead, because the people we serve deserve solutions”



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/>