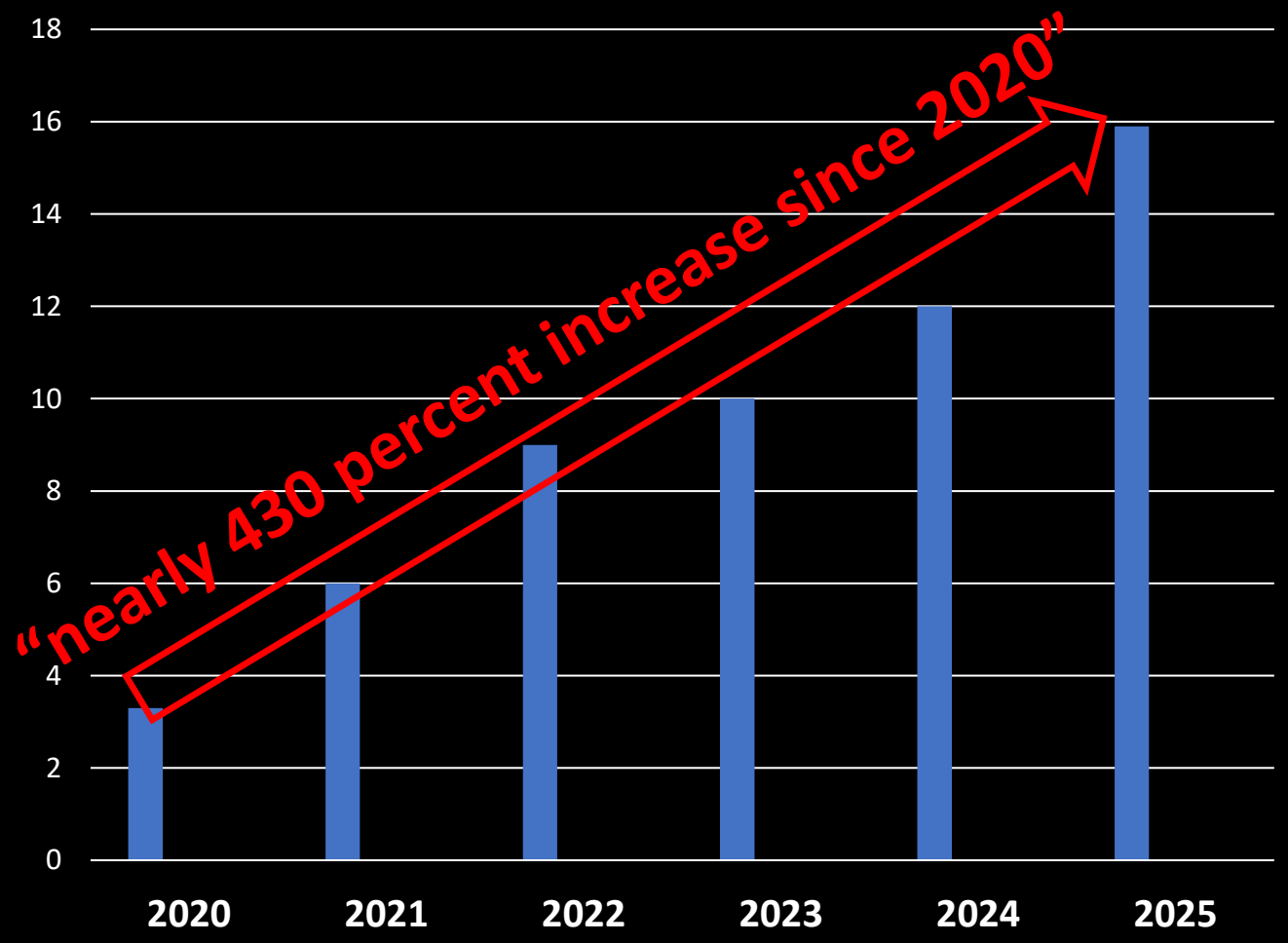
# America Under Scam Attack: Why We Need Stronger Defenses

September 2026

**Ken Westbrook**
CEO, Stop Scams Alliance
Distinguished Fellow, Wilson Center

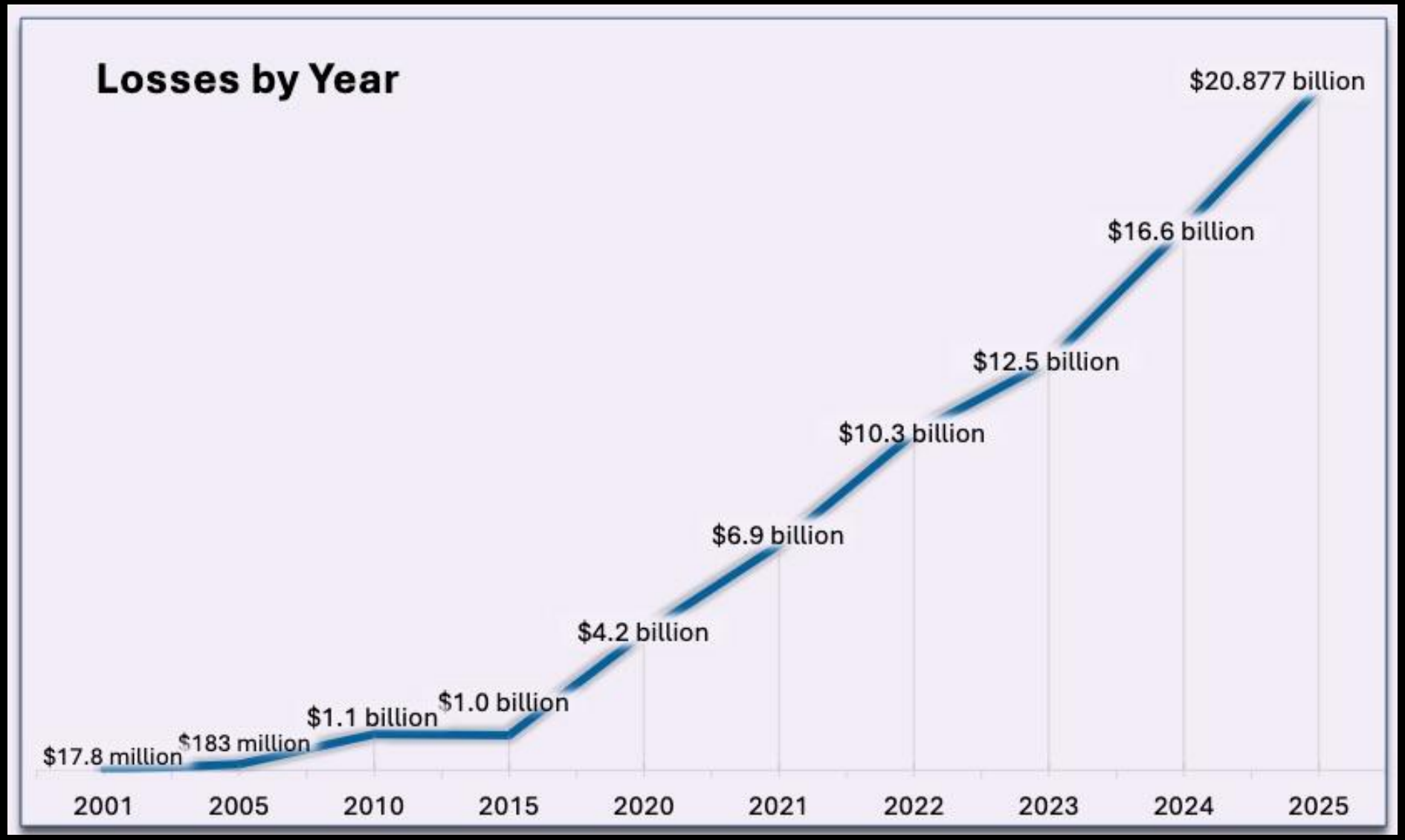


# Fraud reported to the FTC, billions of dollars




https://www.ftc.gov/system/files/ftc_gov/pdf/ftc-testimony-jec-hearing-on-the-rising-scam-economy.pdf

# Cybercrime Losses Reported to the FBI



GALLUP | Stop Scams Alliance




# United States of Scams:

## The Financial and Emotional Fallout

NEW DATA FROM STOP SCAMS ALLIANCE AND GALLUP

Nationally representative
5,173 respondents
Fielded in Jan-Feb 2026

# Estimated losses in 2025, according to Gallup – Stop Scams Alliance Survey




Based on 2025 scams reported to Gallup.



Copyright © 2026 Gallup, Inc. All rights reserved.

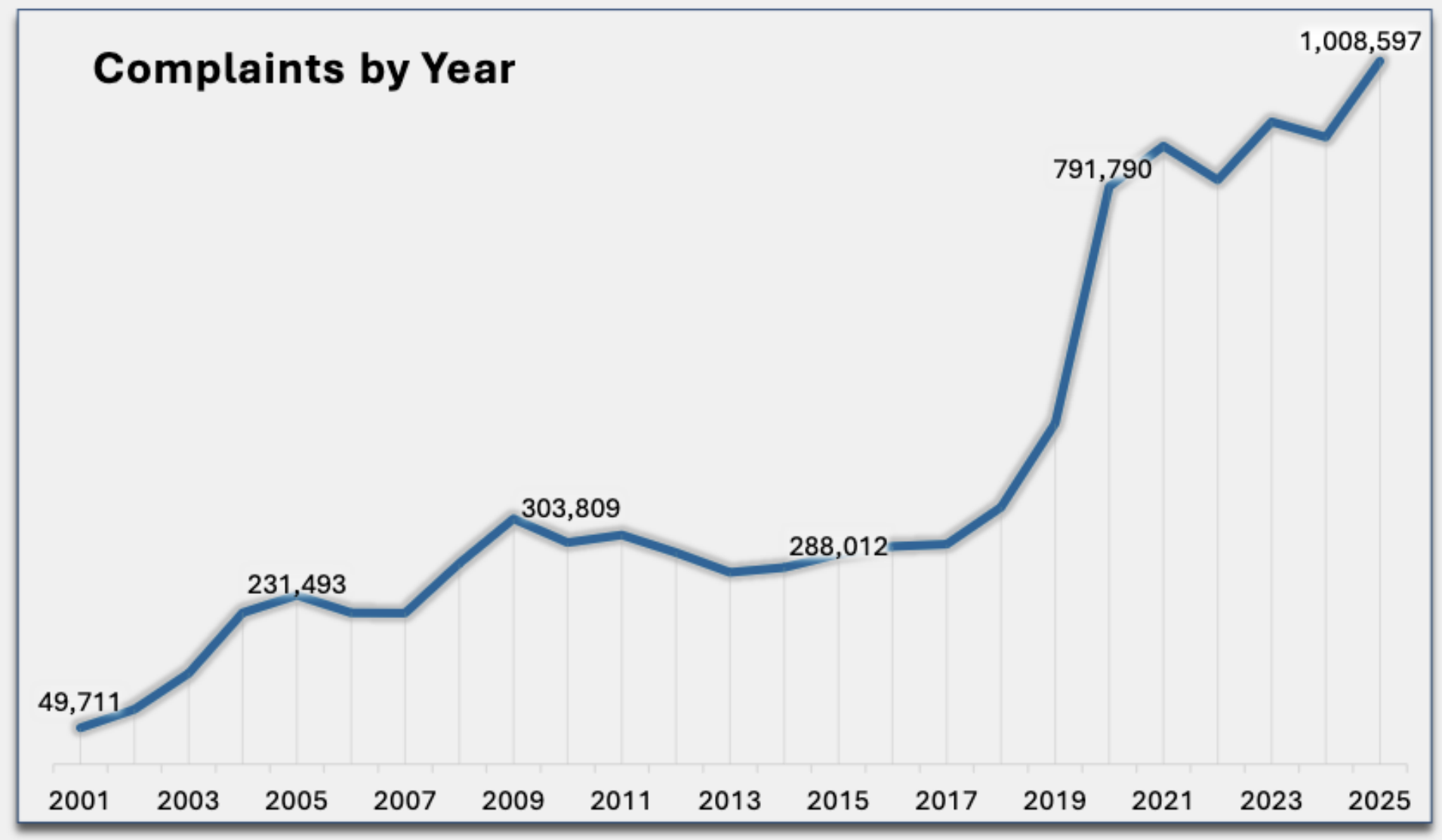
Stop Scams Alliance | GALLUP




Losses reported to government:
$16-20 billion in 2025

Gallup: $68 billion

# Complaints Reported to the FBI



# Results of Gallup – Stop Scams Alliance Survey

- 15.1 million U.S. adults scammed in 2025
- 64 million U.S. adults scammed in their lifetime (One in four Americans)
- 41,000 scammed per day

# 41,000 scammed each day in the U.S.



# INTERPOL expects surge in AI-enabled fraud in next three to five years

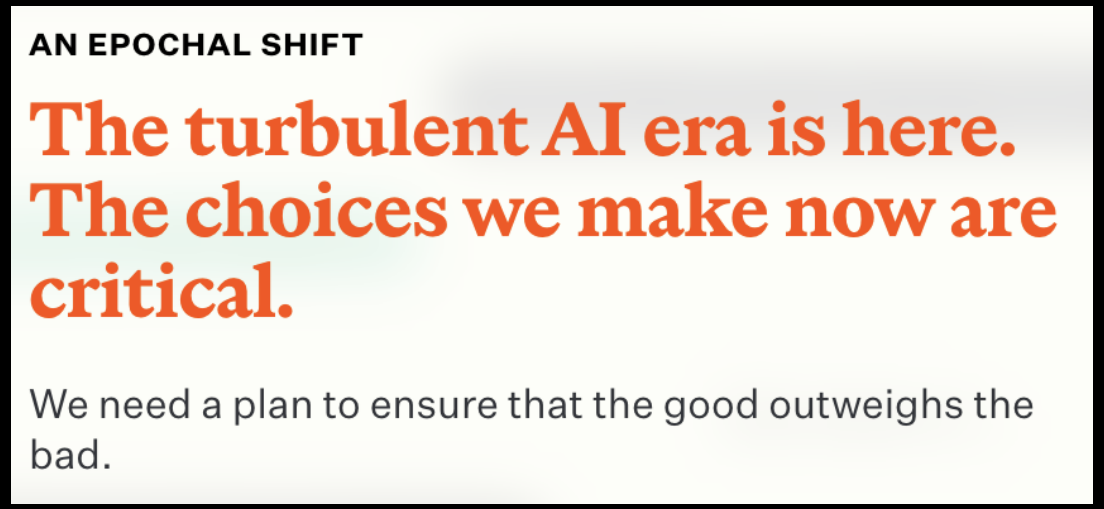



March 2026

"Enabled by artificial intelligence, low-cost digital tools and increased global criminal collaboration, we are witnessing the industrialization of fraud."

"…global surge…notably sextortion, investment scams, impersonation frauds, and fake kidnappings for ransom."

# Bill Gates, 8/26/2026

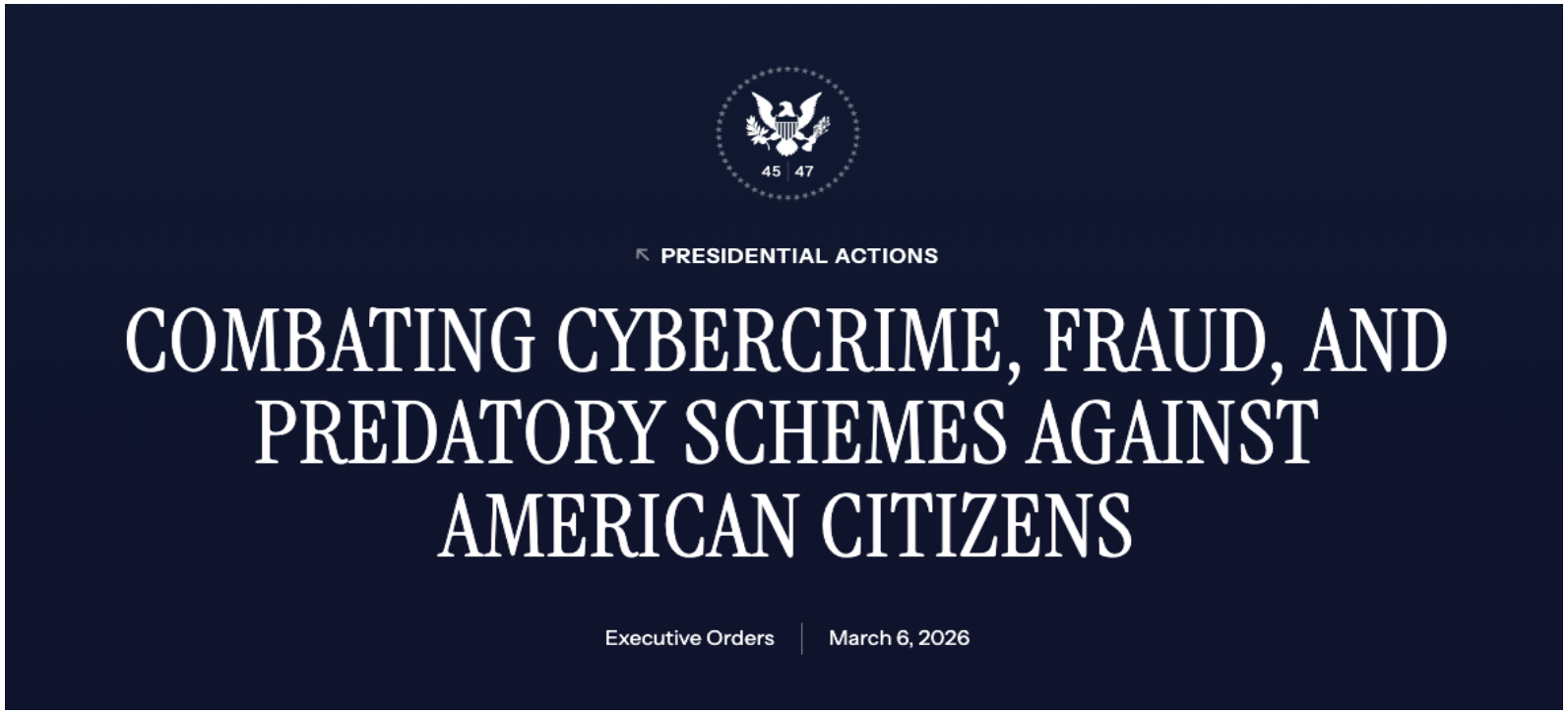

AN EPOCHAL SHIFT

The turbulent AI era is here. The choices we make now are critical.

We need a plan to ensure that the good outweighs the bad.

- “This time really is different”
- “We need time to prepare for the social, political, and economic upheaval”
- “Even criminals with very limited skills will be able to target victims at every scale”
- “AI-enabled fraud, disinformation, deepfakes, and surveillance are the harms that many people will feel most keenly in their everyday lives”

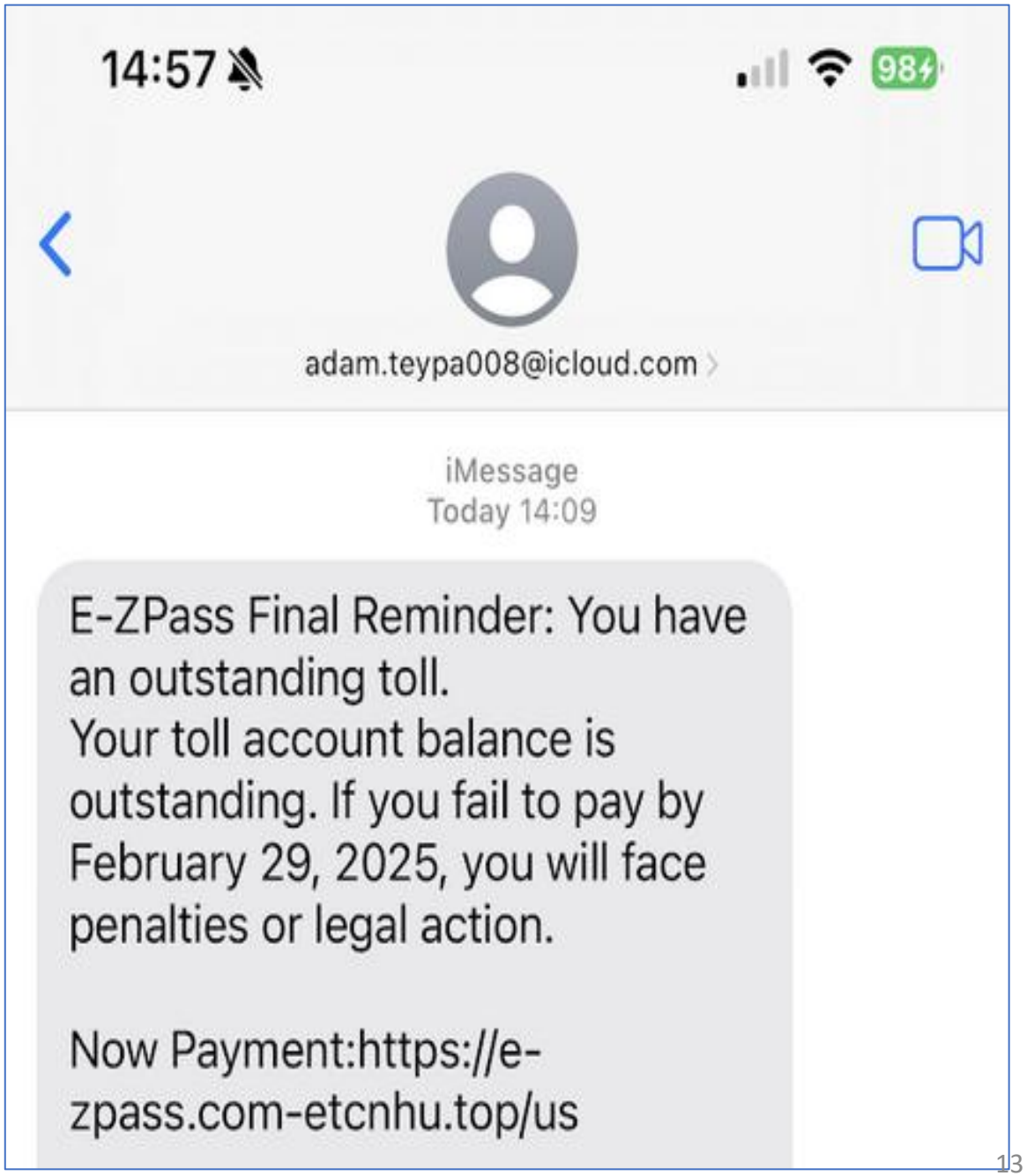
# Who is behind the attack?




"These activities … are often coordinated campaigns carried out by Transnational Criminal Organizations"

UK Government: "persistent threats historically from West Africa, Eastern Europe, India, and China"

Who is sending the toll road scam via text messages?



THE WALL STREET JOURNAL.

EXCLUSIVE CYBERSECURITY

# Chinese Criminals Made More Than $1 Billion From Those Annoying Texts

Messages seeking payment for unpaid tolls prompt victims to hand over credit-card information, which gangs use to buy gift cards and luxury goods

By Robert McMillan Follow

Oct. 14, 2025 10:00 pm ET

Criminal organizations operating out of China made more than $1 billion over the last three years, according to the Department of Homeland Security

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. This is World War 3"*



# A cyber-enabled attack by transnational criminals

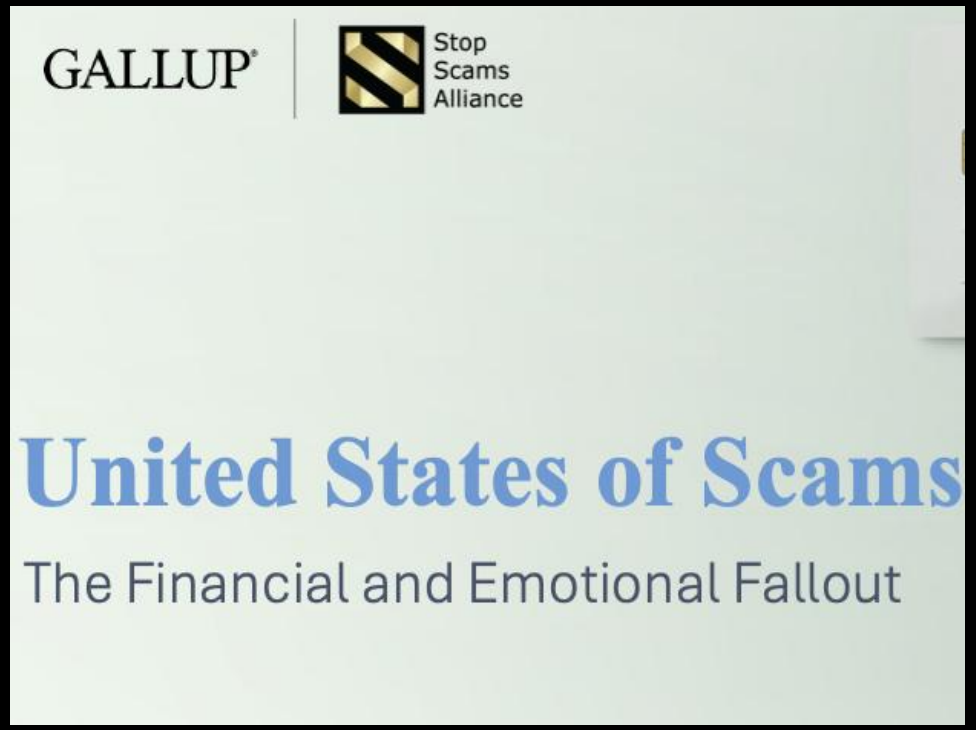
Chinese crime gangs in Southeast Asia: investment scams

India: call center scams

Mexican Narco-terrorists engage in time-share fraud and plow the proceeds into drug trafficking

West Africa and the Philippines: sextortion schemes and business email compromise

# What are the main attack vectors?




Each day, tens of millions of U.S. adults receive a phone call, email, text message or other communication designed to deceive and steal from them.”

# Main attack channels, according to Gallup







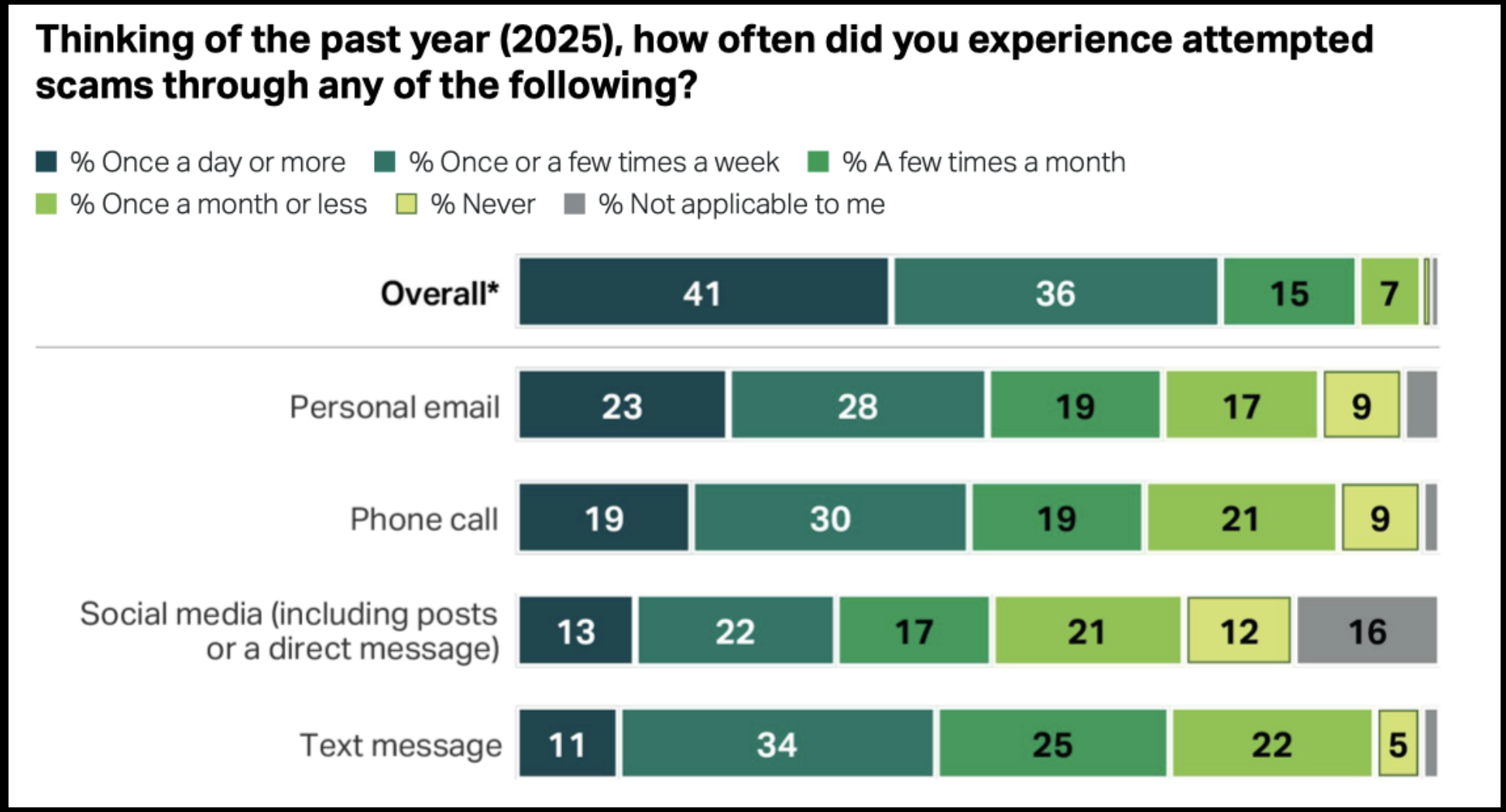
"methods such as phone calls, text messages and emails stand out as most favored by scammers."

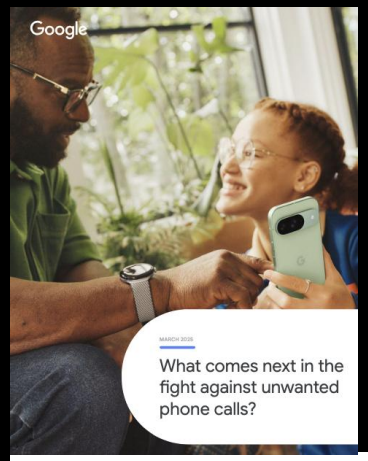





"Fraudulent websites and social media are also commonly used"

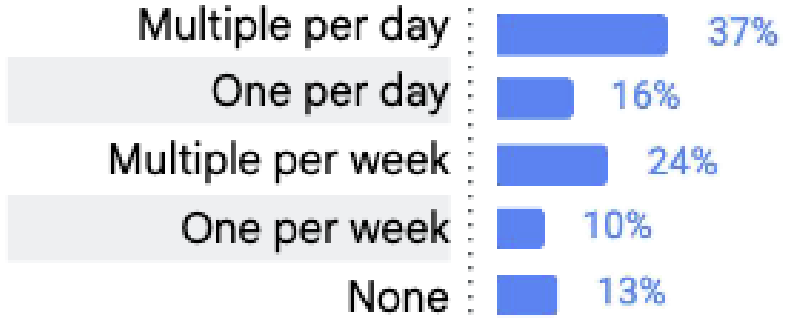
# Americans Are Flooded With Scam Attempts —Four in 10 are contacted daily






# Google/Qualtrics Survey March 2025

***In the past week, how many scam phone calls did you receive?***




Source: Online Survey conducted by Qualtrics on behalf of Google, N=1,961 respondents, US, 18 years or older, Q4 2024

**Unwanted calls have become more than a nuisance, posing a real *financial* and *emotional* threat**

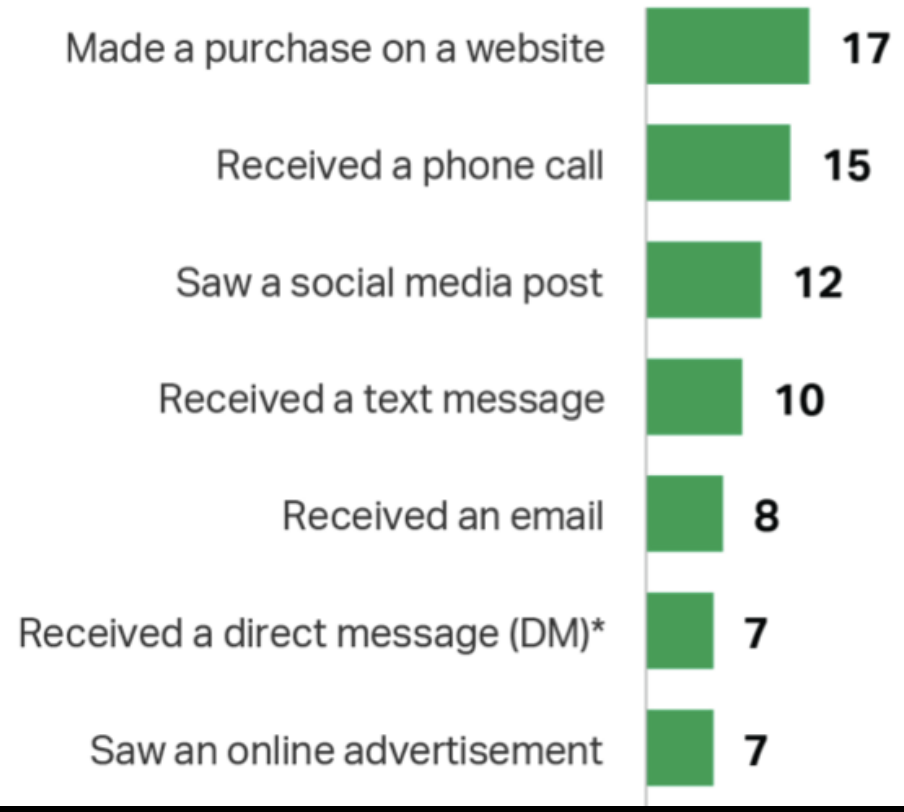
53%: one call per day / 87 % once per week

https://services.google.com/fh/files/misc/2025_phone_by_google_call_scam_report.pdf

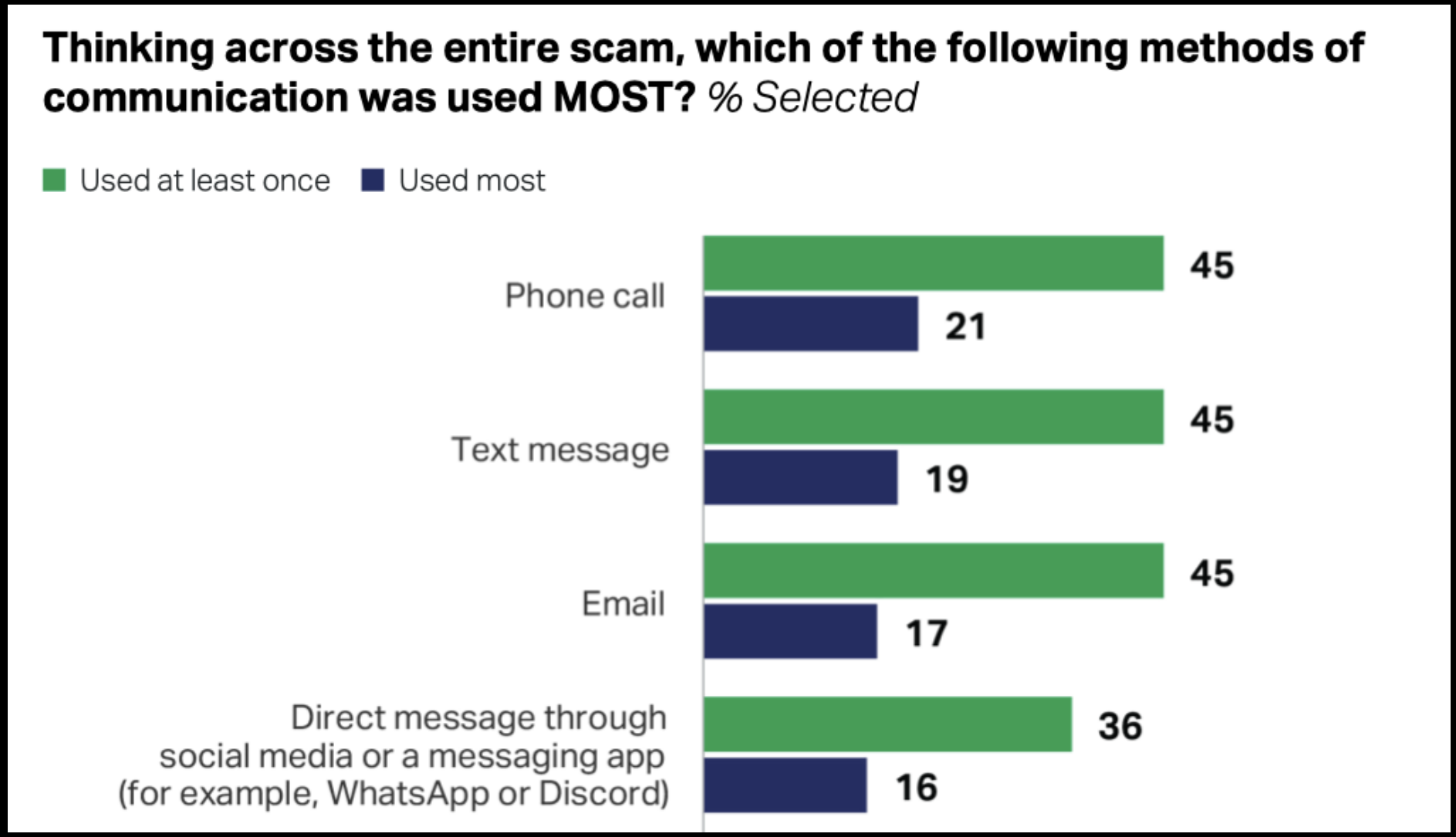
# Online Purchases, Phone Calls and Social Media Rank as Most Common Entry Points

**Which option best describes how the scam first started, at the very beginning? Select one.**

*% Selected*

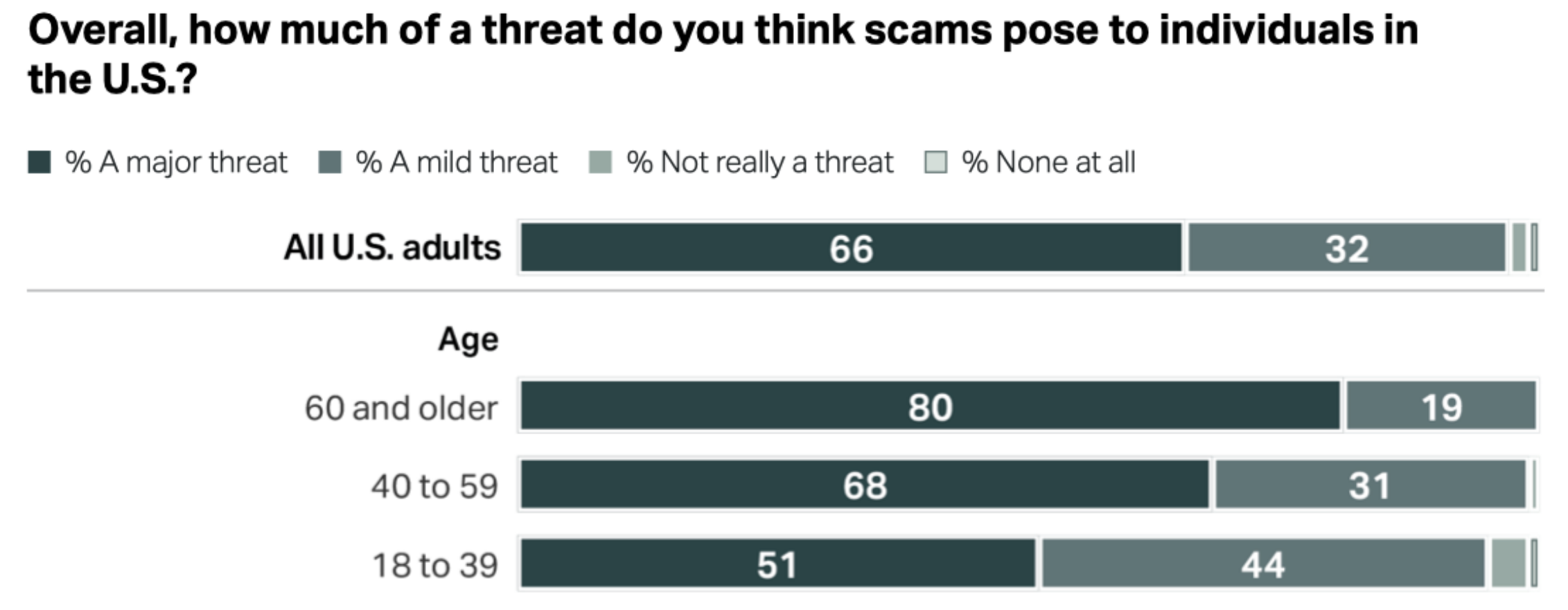


# Phone, text and email each involved in almost half of scams at some point in the interaction




FEDERAL TRADE COMMISSION
A Scammy Snapshot of 2024
(based on reports to Consumer Sentinel)
Big losses follow scams that start with a call or on social media.
Phone calls:
Highest per person reported losses
$1,500
median loss
Social media:
Highest overall reported losses
$1.9 billion
total lost
Email:
Highest overall number of reports
372,000
reports

# 98% of Americans say scams are a threat
# Two-thirds say “major threat”




Stop Scams Alliance | GALLUP

# Responding to a cyber-enabled attack from transnational criminals -- Layered Defense

- Criminal Enforcement
  - Arrests, cyber operations
- Civil Action
  - Google, Microsoft, Meta, PayPal have sued phishing and fake website providers
- Authentication
  - Caller ID, KYC, KYUP, etc.
  - **“No call should be placed onto the telephone network unless it has been authenticated and the party placing it is authorized to do so.”**
- Collection of threat intel, data fusion, blocking

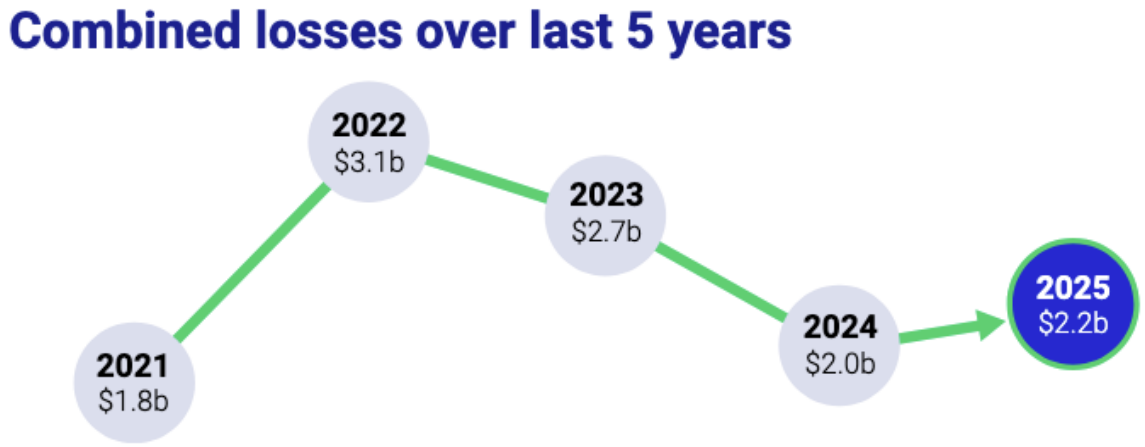
No silver bullet!



# It is possible to bend the curve!

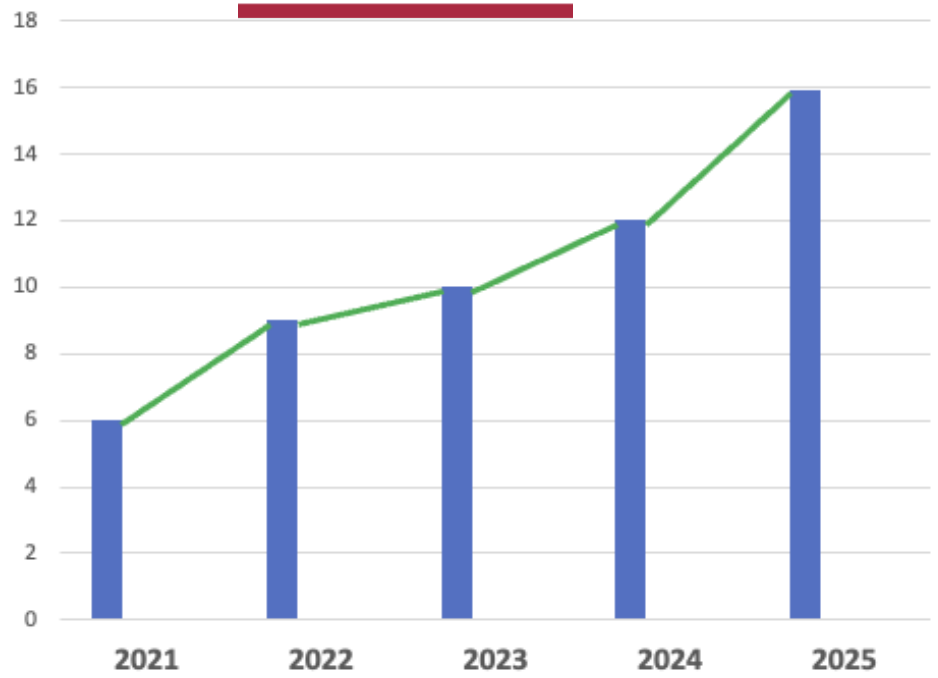
# Fraud losses: Australia vs. the United States






Source: National Anti-Scam Centre






Source: FTC

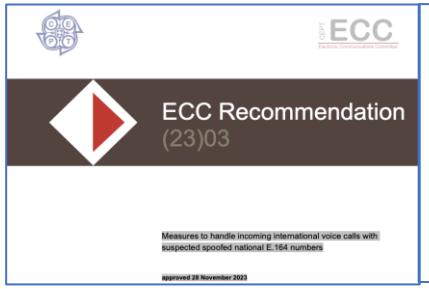
# Nineteen countries block inbound international calls that spoof a domestic number (legitimate call centers exempted)

Starting in 2020-2022:

- Australia
- Finland
- United Kingdom

Starting in 2023 or after:

- Sweden
- Norway
- Belgium
- Latvia
- Lithuania
- Spain
- Czech Republic
- Ireland
- Poland
- Malta
- Romania
- Italy
- Switzerland
- India
- Singapore
- Taiwan




November 2023:
46 countries in the European Conference of Postal and Telecommunications Administrations (CEPT) adopt recommendation to block international calls that spoof a domestic number, or at least strip the caller ID

# Other countries suppress Caller ID of inbound international calls

- **Germany**, **Austria**, and **Switzerland** do not allow an inbound international call to display a domestic number.

- **France** requires that “No caller ID” is displayed when an international call using a French mobile number cannot be authenticated

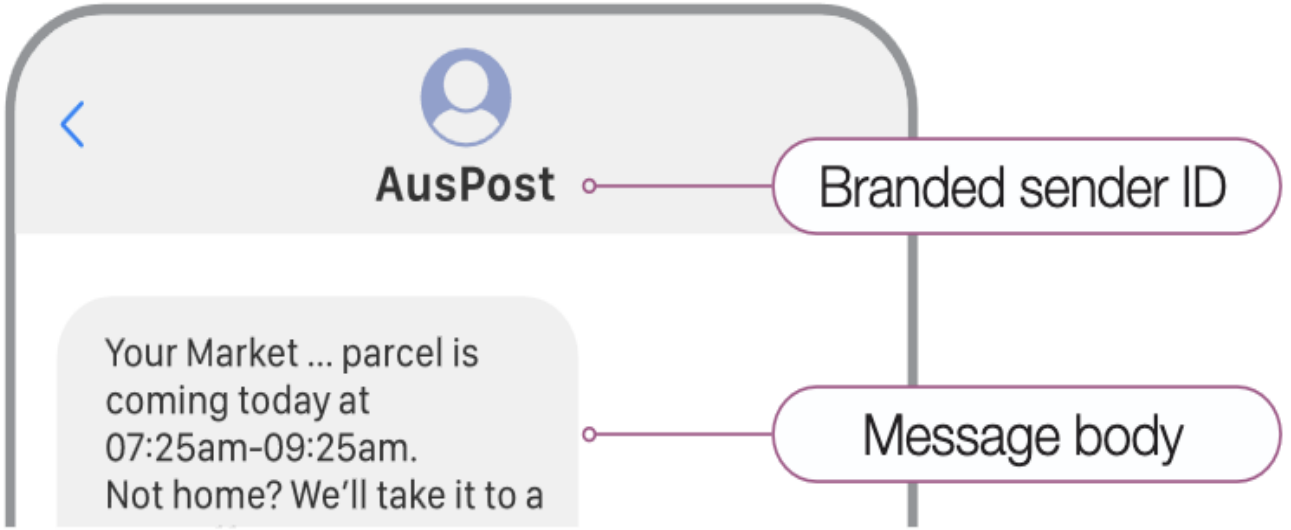
- **Thailand** marks incoming international calls with a "+" sign.

- **Taiwan**’s Chunghwa Telecom plays a voice warning: “Be careful, this is an international call, watch out for fraud”

Australian Government | acma Australian Communications and Media Authority

## Branded SMS Sender ID launched on 1 July 2026

- Messages sent by non-registered telcos and message providers are blocked
- Unregistered sender IDs are labelled '**Unverified**'
- Registered sender IDs displayed




https://www.acma.gov.au/sites/default/files/2025-11/International%20telecommunications%20providers%20-%20SMS%20Sender%20ID%20Register%20fact%20sheet_0.pdf

# “159”

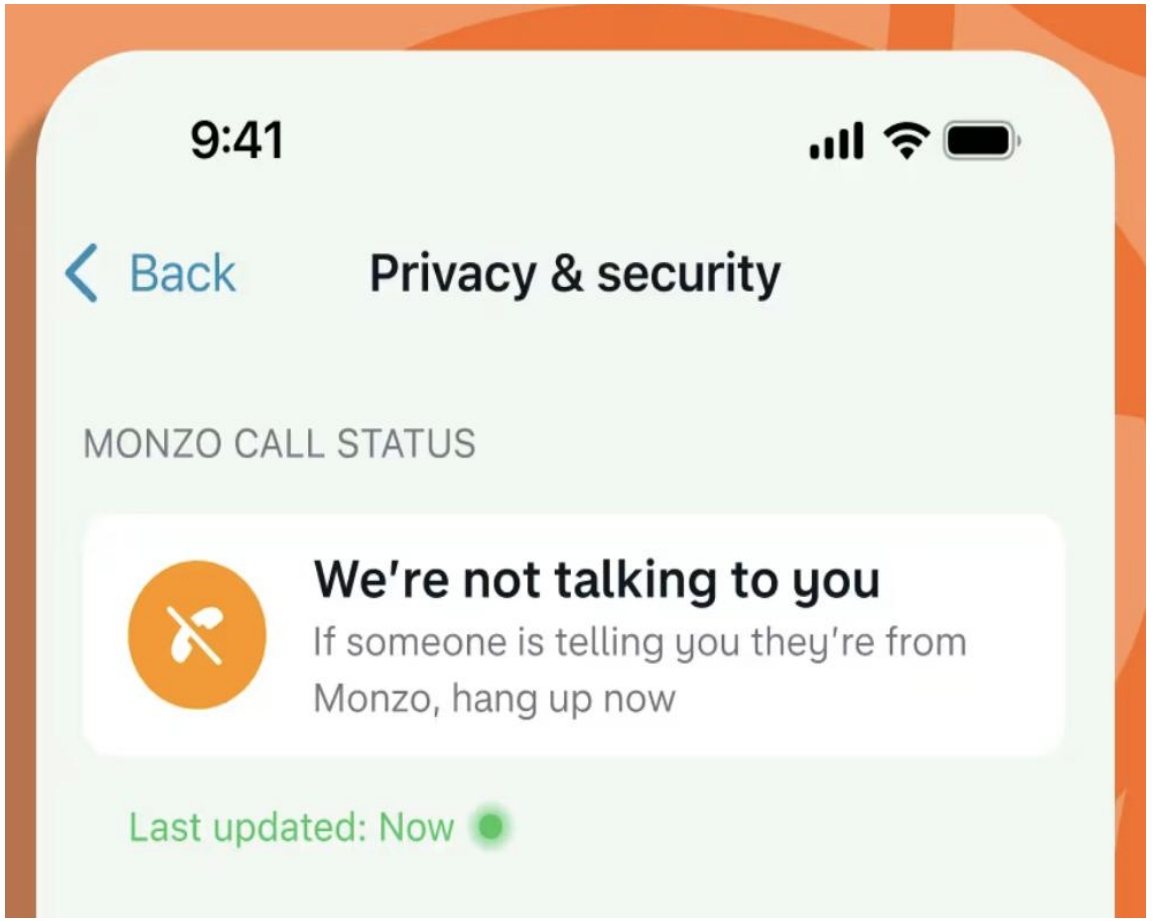
(short-code call-routing service)

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 to 159 since inception (>1,600 per day)

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

# In-App Authentication



# Twelve countries have national anti-scam data fusion hubs

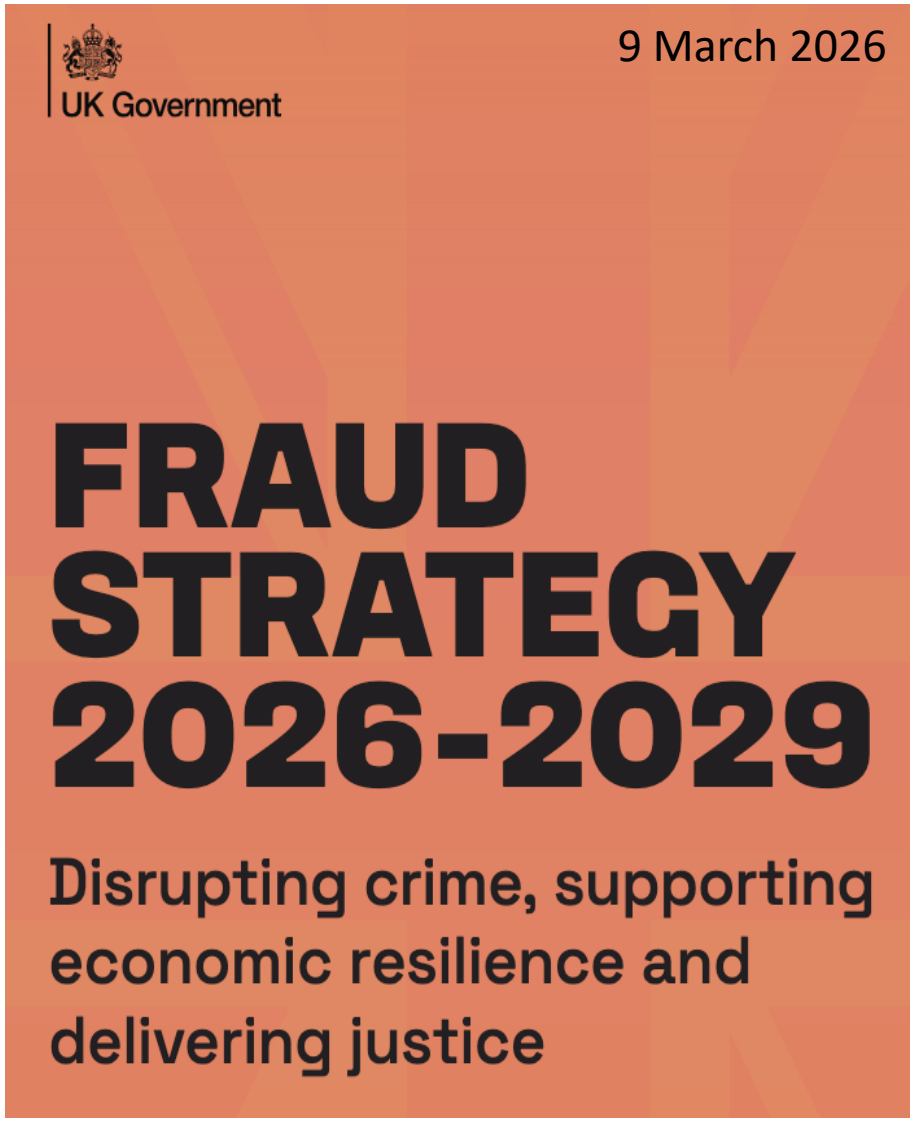
- Singapore (2019)
- Malaysia (2022)
- Saudi Arabia (2022)
- South Korea (2023)
- Taiwan (2023)
- Thailand (2023)
- Australia (July 2023)
- India (2024)
- Indonesia (2024)
- Maldives (2025)
- Canada (2025)
- UK (2026)

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

# In 2026 the Australian government took down

- More than **19,400** scams - an **increase of 182%** since FY25 (fake websites, social media ads, phishing scams and cryptocurrency investment scams)
- 5,476 **phishing scam hyperlinks,** a 279% increase
- 7,051 **fake investment platforms**, a 151% jump
- 3,106 **cryptocurrency investment scams**, a 30% increase

Published 17 August 2026
Source: https://www.asic.gov.au/about-asic/news-centre/find-a-media-release/2026-releases/26-195mr-asic-warns-scammers-are-using-ai-to-spin-vast-webs-of-deception




The Government will invest over £250 million between 2026 and 2029 to combat fraud

£31 million to launch the Online Crime Centre
Began operations in April 2026

Participants:

- UK police
- UK Intelligence Community (including GCHQ, the National Cyber Security Centre and the National Cyber Force)
- Private sector: financial, telecommunications, technology, and cyber industries

Goal: identify and disrupt illicit activities by blocking calls, freezing accounts, taking down websites, and restricting social media accounts


Telecom
Social Media
Financial Institutions
Government



# 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/