



# Stop the Scam! Webinar on Social Media and AI-Powered Fraud

**Marissa Whitehouse**

*Consultant, Alliance for Retired Americans*

**Yosef Getachew**

*Senior Policy Counsel, Reset Tech*

**Alliance for Retired Americans**

**Thursday, January 29, 2026**

# About the Alliance

Founded in 2001 by the AFL-CIO

4.4 million members and growing; 40 state chapters

Members are union retirees and community leaders

Our mission: strengthen retirement security and the health and well-being of older Americans



Robert Roach, Jr., President of the Alliance, testifies before the House Social Security Subcommittee.

# What Is AI?

## How It Works:

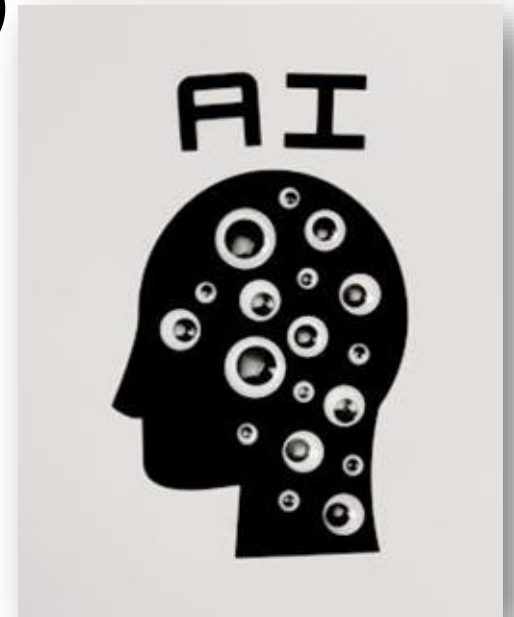
- Trained on huge amounts of data (voice recordings, emails, images)
- Learns patterns in how people communicate
- Generates realistic new content like voices, texts, images

## Examples of AI Today:

- Chatbots that answer like a person
- Voice assistants (like Siri, Alexa)
- Fake phone calls or videos
- Recommendation algorithms on social media

## Why It Matters:

AI can now fake voices, messages, and videos, making scams harder to detect, especially for older adults.



# What is Social Media?

## Social Media:

Internet-based applications and websites that allow users to create, share, and exchange content —including text, images, video, and audio

## Top Platforms by number of users:

[Facebook](#) – social networking; **3 billion** monthly users

[WhatsApp](#) – messaging; **2-2.7 billion** monthly users

[Instagram](#) – photo/video sharing; 2-3 billion monthly users

[YouTube](#) – long and short form video; **2.5 billion** monthly users

[TikTok](#) – short form video; 1.5-1.6 billion monthly users

Others: [X](#) (formerly Twitter), [Pinterest](#), [Threads](#), [BlueSky](#), [Reddit](#)



# Online Fraud and Scams are Reaching Epic Levels

- FBI and FTC data show billions of dollars are lost annually to fraud
- Older Americans are disproportionately affected
  - FBI's Internet Crime Complaint Center Report found that **older Americans reported \$4.8 billion in losses from internet scams in 2024 - +43%** from the prior year
  - Social media was the leading contact method for fraud affecting adults 60 and older, both in volume and in total dollars lost
- Underreporting of scam losses is common due to shame or embarrassment

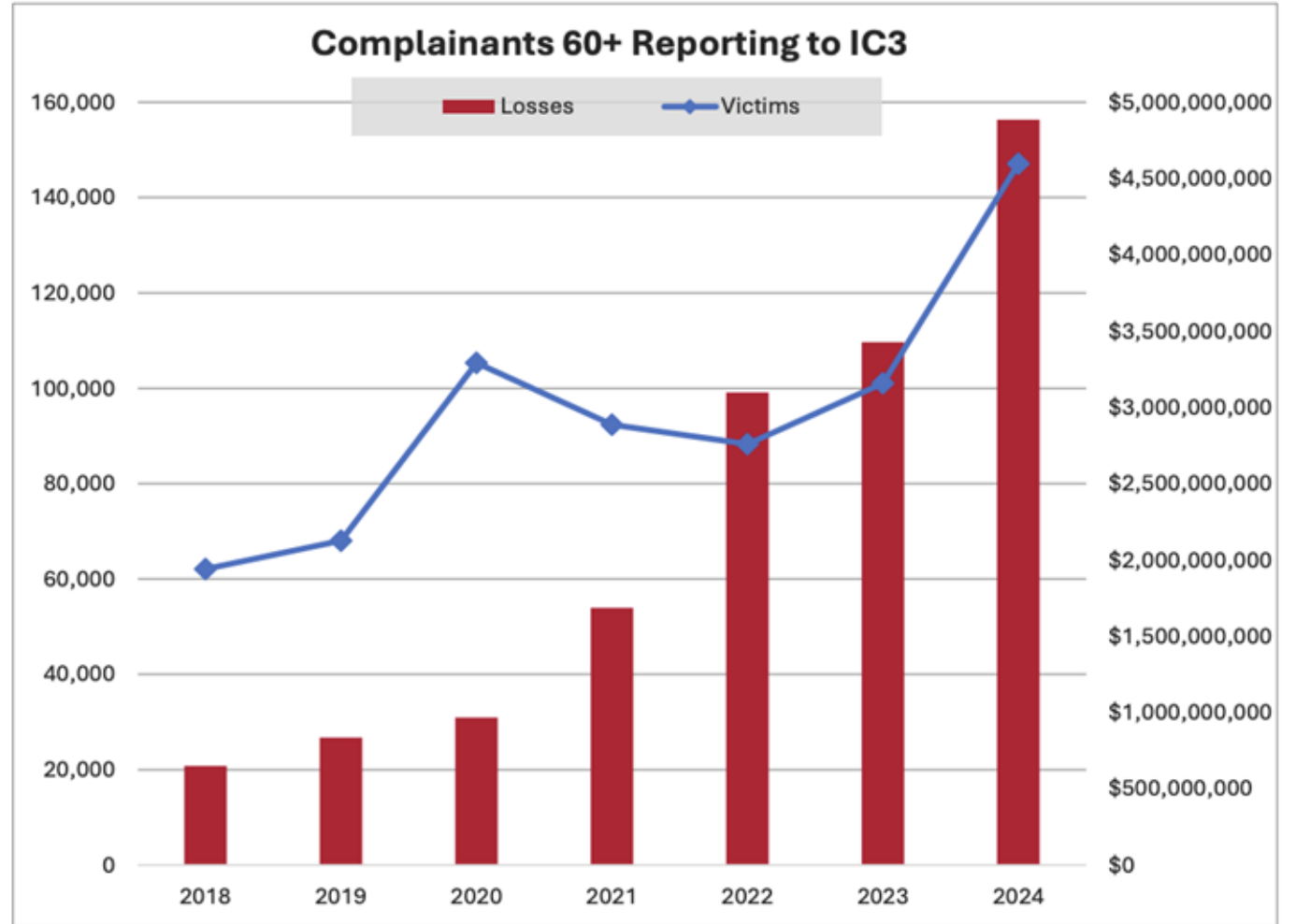
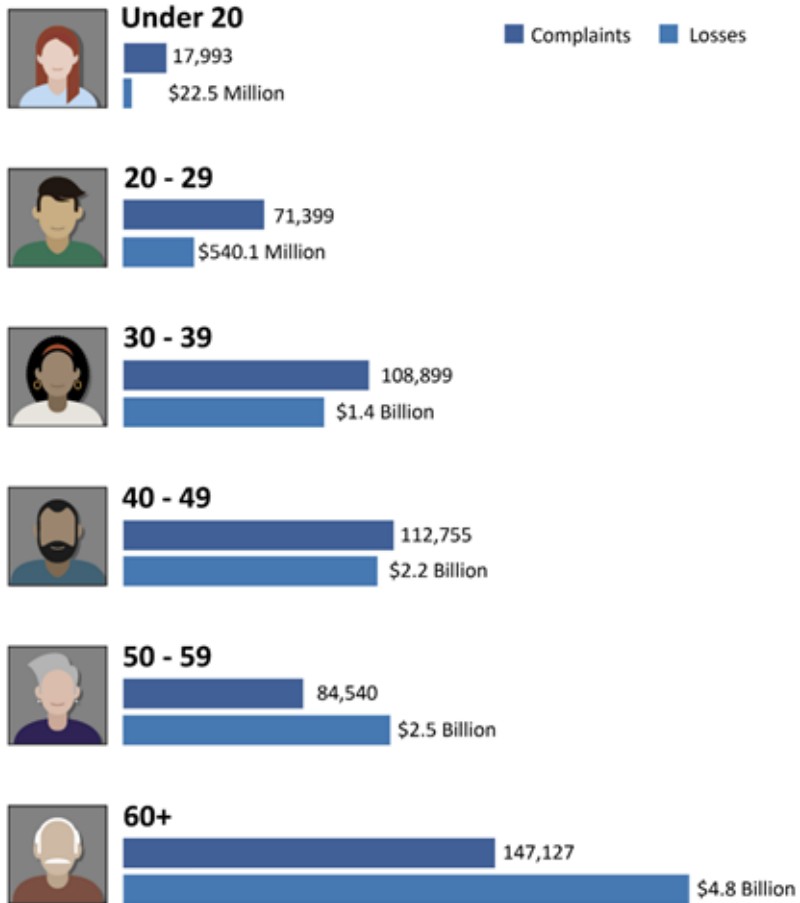


© CBS News

FBI says online scams raked in record \$16.6 billion last year, up 33% from 2023

Apr 27, 2025

# 60+ Hurt the Worst and Getting Worse



All data from 2024 IC3 Report unless otherwise noted

<sup>18</sup> Charts describe count and loss trends for those 60+ from 2018 to 2024.

<sup>19</sup> Accessibility Description: Chart describes counts and losses for those reporting as 60+ from 2018 to 2024.

# Why Older Adults Are Targeted

- High trust in institutions and relationships
- Active online and on social media
- Often targeted for financial resources
- Scams exploit urgency, fear, and trust



# THE VICIOUS CYCLE: HOW AI & SOCIAL MEDIA AMPLIFY SCAMS

## SCAMMERS

Leverage AI to automate and scale fraudulent activities.

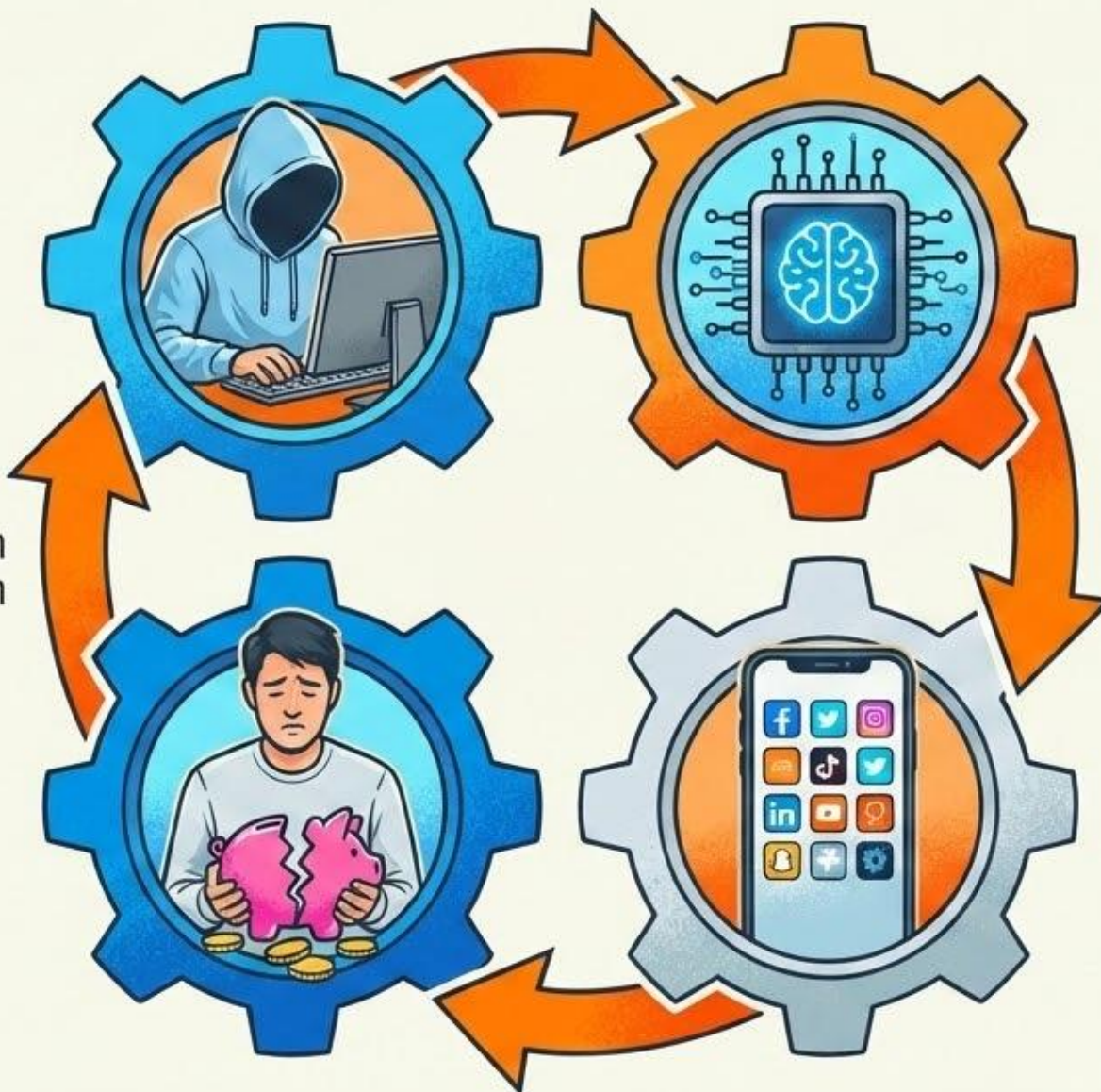
- Increased sophistication & scale.

Funds further investment in AI & platform manipulation

## CONSUMER VICTIMS

Fall prey to sophisticated scams, suffering losses.

- Financial & emotional damage.



## AI TECHNOLOGY

Generates hyper-realistic content, deepfakes, and voice clones.

- Enables personalized deception.

## SOCIAL MEDIA PLATFORMS



Serve as distribution channels with algorithmic reach.

- Vast reach & targeted delivery.
- Scams generate revenue through ads & platform fees.

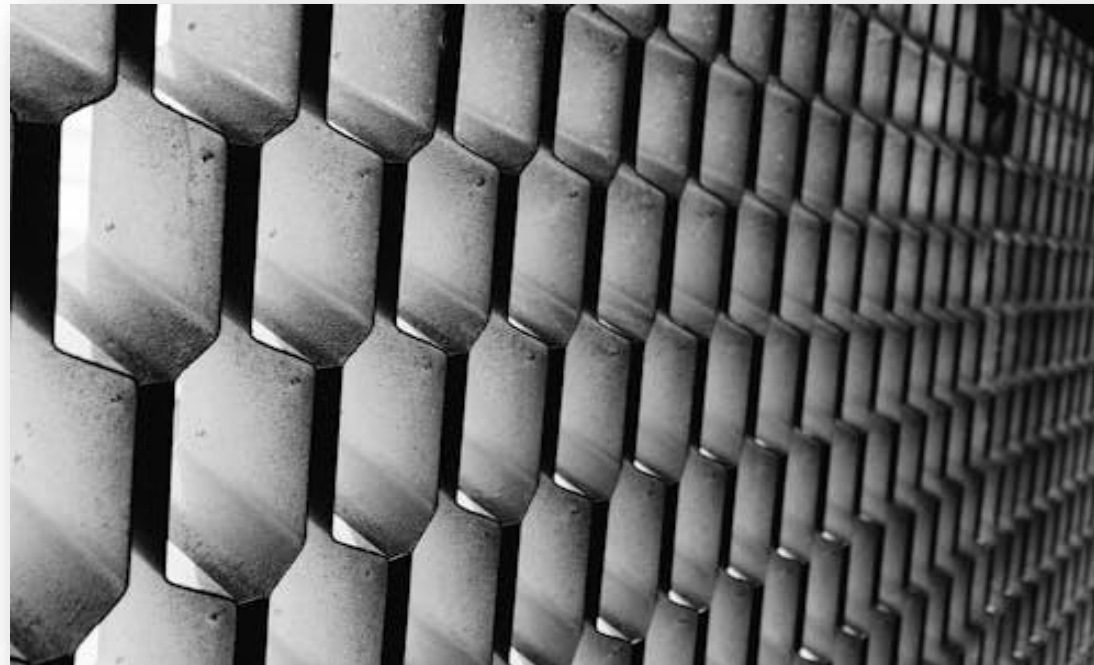
# “Social Media: The Golden Goose for Scammers”



[Click to play video](#)

# Common Scam Patterns

- Impersonation of trusted sources
- Urgent requests for money or information
- Pressure to act quickly
- Discouraging verification
- Unsolicited contact
- Too good to be true



# Real World Example: Grandparent Scams

**Scam:** Using social media accounts to capture grandchildren's voices, scammers use voice cloning software to call grandparents with panicked requests for financial assistance for an emergency situation.

**Impact:** Creates financial harms, but can also leave victims with a sense of shame or embarrassment for having been tricked by sophisticated criminals.

**Example:** A California senior was swindled out of \$25,000 by scammers using an AI voice mimicking his son to make him believe his loved one was involved in a "horrible accident" and needed money to be bailed out of jail. The scammers, posing as his son and later a lawyer, demanded two separate payments to be delivered via Uber driver.



The man, identified only as Anthony, said he received a call from who he believed to be his son, saying he had struck a pregnant woman while driving, and she was "rushed to the ICU,"

ABC 7

# Real World Example: Impersonation Scams

**Scam:** Government impersonation scams thrive on social media where criminals can easily create fake pages or send unsolicited messages to seniors, impersonating officials from federal agencies such as the IRS or Social Security Agency

**Impact:** Recent FTC data shows a more than four-fold increase since 2020 in reports from older adults who say they lost \$10,000 or more from government impersonation scams

**Example:** Scammers created multiple fake accounts and pages on Facebook impersonating government agents to defraud users of nearly \$67 million

© CBS News

Government agent imposters scam Facebook users out of \$67 million - CBS Chicago

# Real World Example: Romance Scams

**Scam:** criminals create fake online profiles to build romantic relationships and exploit emotions to steal money or personal information

**Example:** Kate Kleinert is a Pennsylvania widow who fell victim to a romance scam after accepting a Facebook friend request from a man claiming to be “Tony.”

Over several months of an online relationship, he built her trust and convinced her to send him money, ultimately costing her about \$39,000 of her life savings, pension and late husband’s insurance.



# Real World Example: Health Scams

**Scam:** Scammers buy social media ads to direct people to websites that offer fraudulent health benefits or products

**Example:** Facebook pages are running ads featuring deepfakes or clones of Elon Musk to sell sketchy supplements

Engadget

Facebook scammers want you to think Elon Musk can cure diabetes



# AI is super-sizing this problem

## Consumer Federation of America Report: **\$16 billion in losses - \$5 billion from seniors alone in 2024**

- **Text-based tools**, including chatbots, allow for rapid content creation without obvious spelling or grammar errors, consistent and personalized messaging, and scripts for robocalls and emails.
- **Image-generation tools** are being used for impersonation, extortion, false advertising, engagement-bait, and low-quality AI-generated content across social media feeds.
- **Voice-generation tools** allow scammers to impersonate loved ones or government authorities, bypass voice verification, and escalate romance scams.
- **Video-generation tools**, like deepfakes, are now used in celebrity or government impersonation, extortion schemes, and tech-support fraud.



# Social Media's Role in Enabling Scams

- **Friend requests:** Criminals often send unsolicited friend requests to social media users. Once accepted they can abuse implied trust to push fraudulent content
- **Direct messages:** Criminals send unsolicited DMs to lure users into a conversation, build rapport, and then push fraudulent content
- **Algorithmic recommendations and Targeted Advertising:** Criminals can exploit feeds and “for you” pages to push scam content. Advertising targeting tools and user data can be exploited to push scam ads
- **Groups or community pages:** Criminals can create fake groups (e.g., charity pages, support groups, investment clubs) to cast a wide net in reaching potential scam victims
- **Cloned / fake / impersonated accounts:** Criminals create fake or cloned profiles impersonating friends and family, celebrities, government agencies, politicians, and other public figures to solicit money, personal info, or otherwise push scam content

Social Media  
Platform  
have built a  
business  
model that  
**relies on**  
these frauds  
and scams



## Meta is earning a fortune on a deluge of fraudulent ads, documents show

Meta projected 10% of its 2024 revenue would come from ads for scams and banned goods, documents seen by Reuters show. And the social media giant internally estimates that its platforms show users 15 billion scam ads a day. Among its responses to suspected rogue marketers: charging them a premium for ads – and issuing reports on ‘Scammiest Scammers.’

By Jeff Horwitz

November 6, 2025 6:00 AM EST · Updated November 6, 2025



# “Who is Profiting?”



REUTERS

December 15, 2025

## Meta tolerates rampant ad fraud to safeguard billions in revenue

Internal company documents show Meta wanted to minimize “revenue impact” caused by cracking down on the scams.

[Click here to play video](#)



# Take Action



# Protect Yourself & Your Family

- Slow down
- Verify independently
- Never share personal or financial information
- Talk to someone you trust
- Create a Family Password



# Why Advocacy is Necessary

- Education alone cannot stop industrial-scale scams
- Stronger legal protections and government oversight are needed
- Older adults' voices are critical in policy discussions
- Advocacy can pressure technology companies and policymakers to act



# Platform Accountability and Policy Solutions

- ❑ Pushing back against efforts to pre-empt state AI laws
- ❑ Implement safety by design features
- ❑ Stronger ad transparency and advertiser verification requirements
- ❑ Data sharing with law enforcement and regulators
- ❑ Platform-funded restitution or victim compensation programs



# How to Help: Share Your Story



Storytelling is our **best** tool for advocacy

We will **never** share your story without permission

# Contact Your Representatives



Tell your representatives: don't stand in the way of protecting Americans.

**Send a message** telling them you oppose *any legislation* that pre-empts a state's ability to regulate artificial intelligence and crack down on AI-powered scams.

# Help Us Spread the Word

**Do you know anyone who...**

- Has experienced an AI-powered scam?
- Might encounter a scam?
- Might benefit from this information?
- Would be a terrific trainer?
- Would be a logical partner?



# Questions?

**Marissa Whitehouse**

Consultant, Alliance for Retired Americans

[mwhitehouse@retiredamericans.org](mailto:mwhitehouse@retiredamericans.org)