



October 31, 2026 · Lexington, South Carolina · For immediate release

The \$18 Billion That Walked Out the Door

What Americans reported losing to online fraud in 2025, where the money went, why so little of it comes back, and what to do in the first hours after a scam lands.

On October 31, 2026, TIME reported on a congressional inquiry into what Americans lose to online scams. We went to the primary sources behind that reporting. What follows is drawn from the FBI's Internet Crime Report for 2025. It also draws on the Federal Trade Commission's published estimates, the Joint Economic Committee's report of October 27, 2026, plus United Nations reporting on the scam centers of Southeast Asia. Every figure below is credited to the source that published it.

What the number is

Americans reported losing more than 17.7 billion dollars to online fraud in 2025, according to the FBI. That is more than 2 million dollars an hour, every hour, for a year. It counts only the losses people actually reported. The full count of complaints to the FBI's Internet Crime Complaint Center passed one million for the first time, and total reported losses across all internet crime reached 20.9 billion dollars.

The reported total has climbed every year. It was 12.5 billion dollars in 2023 and 16.6 billion dollars in 2024. The Federal Trade Commission keeps a separate count and watched the same climb in its own reports, from 12.5 billion dollars in 2024 to 15.9 billion dollars in 2025.

And here is the part that reframes everything else. Most victims never report. The FTC studied how many losses its database actually captures and found it catches roughly 2 percent of losses under 1,000 dollars and about 7 percent of larger ones.

Run those rates in reverse and the FTC's high-end estimate of what Americans truly lost to fraud in 2025 reaches 261.5 billion dollars. That is a modeled estimate, not a count. But even the careful version of it says the same thing. The 17.7 billion is the part of the iceberg that filed a report.

Where the money goes

Nearly half of the reported scam losses, 8.6 billion dollars, came from investment fraud. Most of that, 7.2 billion dollars, was cryptocurrency investment fraud, the long con in which a friendly stranger grooms a victim for weeks and then introduces a trading platform that shows beautiful profits and accepts real money. The FBI attributes most of these schemes to organized criminal groups running compounds in Cambodia, Laos, and Myanmar.

Cryptocurrency touched more than 11 billion dollars of the reported losses overall. Business email compromise, the fake invoice and the hijacked house closing, took 3 billion dollars. Tech support scams, in which a fake technician takes over the computer and walks the victim to the bank, took 2.1 billion dollars. Romance and confidence fraud took 929 million dollars, up 38 percent in one year. People over 60 reported losing 7.7 billion dollars, more than a third of everything the FBI counted.

The United Nations adds the human machinery behind the numbers. More than 300,000 people are trapped in scam centers across Southeast Asia, trafficked from at least 80 countries and forced to run these schemes under guard. The person typing sweet messages to a victim in Ohio may be a prisoner in Cambodia. The UN estimates scam losses across East and Southeast Asia, Australia, and New Zealand ran between 88 billion and 114 billion dollars in 2025. America is one market among many.

Why the money leaves so easily

The scam is engineered around one insight. Every step is chosen to make the payment impossible to take back.

Cash sent as cryptocurrency settles in minutes and no bank on earth can recall it. Wire transfers can sometimes be recalled, briefly, if the receiving bank acts before the money hops onward. Crypto ATMs turn physical cash into a stranger's wallet the moment the victim scans a code. Gift cards and mailed cash leave no trail at all.

American law then draws the line in the worst possible place. If a thief steals your password and drains your account, federal rules generally protect you, because you never authorized the transfer. If a scammer spends six weeks becoming your friend

and talks you into authorizing the transfer yourself, the bank followed a genuine instruction from the genuine account holder, and the loss usually stays with you. The scammer's whole craft is moving you across that line, from stolen to persuaded.

The United Kingdom crossed this bridge in October 2024 and now requires banks to reimburse most tricked customers. The United States has debated the same idea for years. It remains a debate.

Why so little comes back

Congress asked the government a simple question this fall. How much of this money do you seize, and how much do victims get back? The answer, in a report released October 27 by Senator Maggie Hassan and Representative Don Beyer through the Joint Economic Committee, is that nobody knows. There is no unified accounting. Each agency counts differently, over different periods, in different categories.

The pieces the agencies did provide are these. The FBI returned 336 million dollars to scam victims in 2025. The FTC delivered 1.83 billion dollars in consumer relief in the year ending September 2025, mostly from domestic enforcement cases, and could not say how much involved the overseas compounds. The Secret Service returned more than 770 million dollars across two years, from all kinds of fraud. The State Department said foreign partners it supports seized proceeds in the low hundreds of millions, and suggested asking three other departments.

Add every named dollar together and it comes to under 3 billion dollars, against more than 17 billion reported lost in one year, with most of it never tied to the compounds at all.

There is one tool that works, and its numbers prove the real problem is time. When the FBI's Recovery Asset Team learns about a fraudulent transfer fast, it runs a process with the banks called the Financial Fraud Kill Chain. In 2025 it froze 679 million dollars, 58 percent of the money in the cases it reached. The Treasury Department says recovery is most likely when a bad wire is reported within 72 hours. The catch is that the team reached 3,900 cases out of more than a million complaints, and most victims learn the truth weeks or months after the money moved. One FBI program phones people whose money is still flowing into scams in progress. Of the 3,780 victims it reached in 2025, 78 percent did not know they were being scammed until the FBI told them.

Even the biggest win comes with an asterisk. In October 2025 the Justice Department moved to seize about 15 billion dollars in bitcoin from the network of Chen Zhi, whose

Prince Group ran forced-labor scam compounds in Cambodia, in the largest forfeiture action in the Department's history. A year later the forfeiture is still not final, and the Department has turned away claims from hundreds of victims who could not prove their specific losses touched those specific coins. Seizing money and returning money turn out to be two entirely different jobs.

What Washington is and is not doing

Some of the response is real. The Treasury sanctioned Southeast Asian scam center networks in September 2025 and designated Prince Group a transnational criminal organization that October. A federal Scam Center Strike Force stood up last November to disable the compounds' infrastructure inside the United States. The Senate has passed the Scam Compound Accountability and Mobilization Act, which would force a national strategy, create a task force, authorize more sanctions, and require the Justice Department to design a way to actually pay victims back. A new law will require dating apps to warn you if someone you talked with was later banned as a scammer. The FTC is considering a rule that would make platforms answer for ads that spread impersonation scams, a category that cost Americans 3.5 billion dollars last year.

What is missing is the front door. The bill that would create one central place to report a scam and get help, and would force the government to run one coordinated strategy, was introduced in June and is still sitting in committee. There is still no single count of what is seized or returned. There is still no right to reimbursement when you were tricked into sending the money yourself. And while the threat spreads, the State Department ended a program that trained police in Bangladesh, a country the UN now flags as an emerging scam hub. The Department says it has the tools it needs. The congressional report disagrees. The victims, meanwhile, get sent from their bank to the police to a website to another website, while the 72-hour clock that decides everything quietly runs out.

The breadcrumbs. How to spot it, slow it, and move fast

Spot the approach. A stranger who wants to move the conversation off the app where you met, onto a private messaging app, within the first day or two. Returns that never dip, on a platform you cannot find in your phone's app store. A small withdrawal that works, offered early, to prove the platform is real. Then, when you try to take out real money, a tax, a fee, or a verification deposit you must pay first. Anyone who coaches you on what to tell your bank. Anyone who needs secrecy and speed at the

same time. A voice that sounds like your grandchild, your boss, or your bank, asking for money in a way that cannot wait for you to check.

Slow it down. The single rule that defeats most of it is this. You cannot free your own money by sending more money. A real investment never charges a fee to release your balance. Leave the chat and call the institution on the number printed on your card, never a number the other side gives you. Say the firm's name out loud to one person who is not in the conversation, and search the name with the word scam after it. If a bank employee asks why you are withdrawing, answer honestly. That question has saved more retirements than any software. Pressure is the tell. Anything that cannot survive you sleeping on it is not an opportunity. It is a countdown the scammer set.

If it lands, the first hours decide it. Call your bank immediately and use the exact words recall and freeze. Ask what they can still stop, and write down the name of everyone you speak with. File a report at ic3.gov the same day, with the full transaction details, wallet addresses, account numbers, dates, and amounts. That report is what can trigger the FBI's freeze process, and the Treasury Department puts the practical window at 72 hours. Report it at ReportFraud.ftc.gov as well, and tell your local police, because some banks and insurers want that report number. Save everything. Screenshots, transaction receipts, the phone numbers and account names, all of it.

Then expect the second act. People who have already lost money are targeted again by fake recovery agents, fake law firms, and fake officials, sometimes posing as the FBI itself, offering to recover the loss for a fee. In 2025 those recovery scams took another 1.4 billion dollars from people who had already been hurt once. Nobody legitimate charges you up front to return your own money. The government will never ask for a fee, a gift card, or a crypto payment to release seized funds. If the offer to help arrives before you asked for it, it is the same crime wearing a rescue vest.

The honest bottom line

The 18 billion dollar headline is not the size of the theft. It is the size of the reported theft, the slice of victims who overcame the shame and found the right website. The people running these schemes have solved their side of the problem. They have free distribution, forced labor, patient scripts, and payment rails that do not reverse. The American side is still a relay race in which no runner owns the baton. Until the reporting has one door, the losses have one honest count, and someone is assigned to own the seams between the platform, the phone company, the bank, and the

exchange, the number in next year's headline is already being decided, in compounds most Americans will never see, one friendly conversation at a time.

SOURCES

FBI, Internet Crime Report 2025, released April 6, 2026, figures of the Internet Crime Complaint Center. Federal Trade Commission, fraud loss estimates published October 2026. Joint Economic Committee, minority report released October 27, 2026. United Nations, reporting on scam centers in Southeast Asia, 2025. The figure of 261.5 billion dollars is the Federal Trade Commission's modeled high end estimate, not a count, and it is labeled as an estimate where it appears.

Contact. Agentic Armor LLC · contact@agenticarmorllc.com · agenticarmorllc.com

The canonical text of this release lives at <https://agenticarmorllc.com/releases/cyberscam-losses-2026/> and the release library stands at agenticarmorllc.com/releases/.