Not long ago, Monica Cotelingham found herself stuffing cash into a Bitcoin machine at a gas station in suburban Maryland and weeping.

Earlier that day, she had received a call from a phone number with the same area code as Cotelingham's father in Louisiana. When she answered, someone identifying themselves as a U.S. customs officer said the government had found a package addressed to Cotelingham that contained stolen passports and driver's licenses. She was in a lot of trouble; law enforcement was going to call her back. When Cotelingham's phone rang next, the number that came up was from local police, who told her the FBI would be in touch. Minutes later, she got a call from a number that matched the bureau's. The person on the line told Cotelingham that she could get out of the mess by depositing $18,000 into a Bitcoin machine.

In retrospect, Cotelingham says, she should have known it was a scam. The game of law-enforcement telephone made no sense. All the callers had heavy accents. Each instructed her not to tell anyone what she was doing. The bank teller at Truist, where she withdrew the $18,000, asked if Cotelingham was OK, and warned her of scams. Even the Bitcoin machine where she deposited the money had a warning, in big red letters, to beware of scams and fraud. But Cotelingham, who received the calls on her first day of a medical leave of absence from her job as a psychiatrist, believed at the time that they were legitimate. And so, sobbing in distress, she stuffed $10,000 into the machine until she asked the clerk for help to stop. "Even then, I think part of me knew," she says. "It was incredibly traumatic."

Cotelingham's experience is increasingly common. We are living in the golden age of scams. U.S. consumers lost a record $10 billion to fraud in 2023, according to the Federal Trade Commission, a 14% increase over 2022. That tally is almost certainly an undercount. More than three-quarters of victims, including Cotelingham, don't report to authorities that they've been defrauded. We are constantly baited by scammers—by text, by email, by phone. The average smartphone owner in the U.S. gets an estimated 42 spam texts and 28 spam calls per month, according to RoboKiller, an app for screening calls.

The scams themselves are more sophisticated than ever before, capable of duping the most skeptical consumers. There are romance scams, investment scams, and fake-job scams. Scammers target everyone from pharmacists in Wisconsin (trying to persuade them to send money because their credentials have supposedly expired) to employees of specific companies (sending emails or texts that say they're from the CEO and instructing employees to buy gift cards). "We are at an epidemic level of fraud," says Kathy Stokes, director of fraud-prevention programs with AARP.

The COVID-19 pandemic is one reason. It made people lonelier and more isolated, which research shows makes them more susceptible to fraud, and it pushed more transactions online, where we can more easily fall victim. One in 3 Americans experiences feelings of loneliness at least once a week, according to a recent poll from the American Psychiatric Association. Members of Gen Z are more anxious and depressed than previous generations—and three times as likely to fall for scams as baby boomers.

But there are other factors. Technology enables scammers to reach more marks, robo-dialing many more numbers in a day or using AI to send carefully crafted emails and text messages. It's also given rise to online marketplaces selling hacker services, scam scripts, and other tools of deception. Social media helps scammers find information about individuals and use it against them. And fraudsters have more of that information because of increasingly common data breaches, and can use it to trick us into thinking they're someone they're not.

That specific kind of grift is known as an impostor scam. A perpetrator reaches out, pretending to be a government official, a bank representative, or a law-enforcement agent. Impostor scams like the one Cotelingham fell victim to were responsible for nearly half of all frauds reported to the FTC in 2023, with about 490,000 people reporting them. Americans said they lost $1.1 billion to impostor scams last year, three times what they lost in 2020. The success of the impostor scam illuminates another reason criminals are able to bilk Americans today. Our trust in institutions has collapsed, making it easier for scammers to pose as authority figures, says Stacey Wood, a fraud expert and professor at Scripps College in California. "Authority can look very different now," Wood says. "If someone is skeptical of the U.S. government, they often trust someone else—who can scam them."

Americans may not believe in the government or the media, but we want to believe in something—and sometimes that's a stranger who says they can solve our problems, or love us, or give us our dream job, or take our money in exchange for a better life.

Doug Shadel, a fraud expert and consultant who recently directed AARP's Fraud Watch Network, has fought scammers since the 1990s. Back then, employed by the Washington State attorney general's office, he used to bust so-called boiler rooms—places where dozens of people made scam calls, reading from prewritten scripts and dialing numbers one by one. The scammers might reach a few hundred people in a day, Shadel says, and would have to pay long-distance charges for the phone lines. Now, Shadel says, voice over internet protocol (VOIP) technology allows scammers anywhere to dial hundreds of thousands of phones in a day for free—what Shadel calls "spray and pray" dialing. They can "spoof" phone numbers, making it look like they're calling from a government number. And they know much more about who they're calling than ever before.

There were 3,205 reported data breaches impacting around 353 million people in 2023, according to the Identity Theft Resource Center. As a result, many of our Social Security numbers, addresses, phone numbers, or affinity-group memberships are available to resourceful scammers. One California family, who requested anonymity for fear of being bilked again, lost $400,000 when a scammer, armed with one of their Social Security numbers, called Bank of America 16 different times to try to change the password and information on an account, according to the family's lawyer, Nick Barthel. Fifteen bank representatives refused, but the 16th was duped, according to Barthel, who says the scammer wired the family's savings out of the account. The bank has not refunded the family, Barthel says. (Bank of America says it cannot comment on pending litigation. Police eventually found the perpetrator, but he was

deceased and the money was nowhere to be found.) “This could happen to anybody,” says Barthel. “All the guy needed was the basic information you would get from a data breach.”

This data often finds its way onto messaging apps like Telegram, says Frank McKenna, co-founder of PointPredictive, an AI firm that detects frauds. Cybercriminals can buy and sell tutorials and scripts for scamming people, as well as victims’ personal information. For $500, you can purchase a live scamming class, 25,000 U.S. phone numbers, and instructions for sending spam links, according to a report from the security firm Guard.Io. “Social media platforms like Telegram began to emerge as these hubs of scam knowledge and transfer,” McKenna says. (Telegram CEO Pavel Durov was taken into custody in Paris on Aug. 24 and faces charges stemming from the platform’s alleged role in enabling criminal activity; Durov calls the charges “misguided.”)

Scam syndicates exist all over the world, from Southeast Asia to Mexico to the Middle East, says Marti DeLiema, a professor who studies scams at the University of Minnesota’s School of Social Work. “This is the new mafia,” DeLiema says. The work can be lucrative. A 2024 report by the U.S. Institute of Peace found that transnational criminal networks based in Southeast Asia steal $64 billion annually through scams. In Myanmar, according to the report, there are “scam compounds” where people who have been lured by fake online job ads are held prisoner and forced to make calls to try to swindle Americans.

The rise of artificial intelligence has been a boon for these scammers. A decade ago, you might have been the target of a poorly written email from someone claiming to be a Nigerian prince and asking for money to help them regain access to their wealth. Today, AI helps non-English speakers write more convincing missives. The technology can also be used to copy voices and likenesses to convince people that their family members are in danger. That’s what happened to Fauzia Vandermeer.

Vandermeer, a 51-year-old radiologist who lives in Baltimore, received a call earlier this year from a number she didn’t recognize. She ignored it, but the person called again, so Vandermeer picked up, worried that something had happened to a family member. She heard the sound of her sister’s voice, sobbing and asking for help.

“I was totally freaking out,” Vandermeer remembers. The voice that resembled her sister’s told Vandermeer that she was at a Walmart and had gotten into an accident. Then a man came on the line. He said that Vandermeer’s sister had hit his van, which had kilos of drugs in it, and that he needed to be compensated. Vandermeer was in her car, ready to drive to the Walmart, when the man told her that the matter needed to be dealt with “sensitively,” she says. Suspicious, Vandermeer asked one of her children to try to locate her sister, which they did with the Find My Friend function on their iPhone. Vandermeer’s sister was at home. Vandermeer sidestepped the scam, but says she easily could have been victimized. “To hear a loved one on the phone, crying for help,” she says, “immediately you are kicked into this stress response.”

People are more likely to fall prey to scams when they are in a heightened emotional state. That's why scammers try to target your emotions, telling you that you've won some sort of prize or money, or that something terrible has happened. It's a big reason people get duped by frauds that strike observers as obvious. A 2021 AARP study found that scam victims reported experiencing twice as many stressful life events in the past year as nonvictims.

The Department of Justice says it has stepped up efforts to catch and prosecute scammers who target Americans, even when those criminals are in other countries. From July 2022 through June 2023, the department says it pursued 300 criminal and civil actions against more than 650 defendants who collectively stole more than $1.5 billion from over 2.4 million victims. U.S. authorities also partner with foreign law-enforcement offices. One such collaboration last year led Indian police to raid call centers, arresting 26 people and seizing equipment used in scamming, according to a senior DOJ official, who says a similar effort is under way in Ghana.

Some people, frustrated with the government's inability to combat scammers, have taken on the task themselves. They're known as scam baiters, and they embrace a kind of vigilante justice—working to lure the scammers into targeting them and then hacking into their computers or collecting evidence they can turn over to authorities.
One such scam baiter is Jim Browning. He's an IT specialist in Ireland who got frustrated by the bombardment of scam calls and emails he was receiving. Browning, who uses a pseudonym, tries to catch scammers and turn them over to authorities, as well as to educate viewers on his YouTube channel, which has 4.3 million subscribers. His technological prowess offers him—and his viewers—insight into who the perpetrators are and how their operations work. In one of his most-watched videos, Browning accesses CCTV camera footage to watch Indian scammers run the same grift that duped Monica Cotelingham. The footage shows young men sitting in cubicles in a call center, dialing potential victims until eventually one finds a mark. The scammer instructs the target to deposit money into a Bitcoin machine before passing the phone to his superior—a "closer," Browning explains, someone with better English and more experience.

Browning's channel illustrates how hard it is to stop people from being scammed, even when they're made aware that a crime is unfolding. In the video, Browning hears where the scammers tell the victim to deposit the money, calls the location—a store in Michigan—and reaches a clerk. Browning tells the clerk that the woman stuffing money into the store's Bitcoin machine is being scammed. The clerk acts quickly, passing the information on to the woman. But she can't be deterred. "She's not budging on thinking that it's real," the clerk tells Browning. It's also why Browning, who has worked as a scam baiter for a decade, is skeptical about law enforcement's ability to counter fraudsters. "I have encountered thousands of scam operations," he says, "and the percentage of people who actually get arrested is tiny."

Another scam baiter, an American who uses the alias Kitboga, tries to torment or prank the scammers as a form of payback. Kitboga, who has 3.6 million subscribers on YouTube, will give scammers access to his computer and then go into theirs to delete files. He says he takes these steps because law enforcement isn't equipped to deal with all the scammers out there and he wants to educate people about the risks. "This is," he says, "a pandemic-type situation."

Pierogi, the nom de guerre of a popular YouTuber who runs a scam-baiting channel called Scammer Payback, says he has started feeding federal authorities information about scam rings. "All different sorts of agencies have knocked on my door," says Pierogi, a onetime cybersecurity expert who adopted the pseudonym because his wife is Russian. (Yes, he knows pierogi are Polish.) Yet even when police get involved, it can be hard to put scammers away. A conviction can require law-enforcement cooperation across multiple countries and victims willing to testify. Scammers sometimes still escape with just a slap on the wrist. "We're making it harder for the scammers, but they're also getting smarter," Pierogi says. "It's this cat-and-mouse game."

The true toll of these scams goes far beyond the financial losses. In the age of scams, consumers are stuck in a vicious cycle: a lack of faith in institutions makes us fall victim to fraud, which in turn makes us even less trusting of institutions. Monica Cotelingham is still reeling from the scam that targeted her in 2022. She says she's less trusting and never answers her phone if it's not someone in her contacts. "I'm very careful about what information I reveal," she says. She was too trusting just once, she says—and now she finds it difficult to believe in anyone at all.

Correction appended, Sept. 18*: The original version of this story misstated the pseudonym of a scam baiter; he goes by Kitboga, not Kit Boga. It also misstated whether he has teamed up with other scam baiters to send glitter bombs; he has not.*