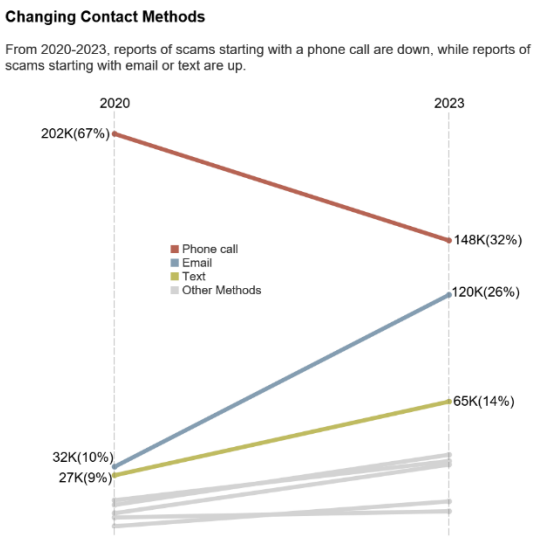
April 2024

Consumer Protection Data Spotlight

FTC reporting back to you

Impersonation scams: not what they used to be

Scams that impersonate well-known businesses and government agencies are consistently among the top frauds reported to the FTC's Consumer Sentinel Network.[1] In 2023, data from the FTC alone show more than 330,000 reports of business impersonation scams and nearly 160,000 reports of government impersonation scams.[2] That amounts to nearly half the frauds reported directly to the agency.[3] Combined, reported losses to these impersonation scams topped $1.1 billion for the year, more than three times what consumers reported in 2020.[4]



Figures are based on the total number of reports to the FTC Consumer Sentinel Network classified as business imposter or government imposter. Reports provided by Sentinel data contributors and reports that did not indicate a contact method are excluded.

While these types of scams aren't new, reports tell us scammers have switched things up. Comparing 2020 to 2023, for example, reports of scams starting with a phone call have plummeted, while reports of scams starting with a text or email have increased. In that same period, people reported skyrocketing losses through bank transfer[5] and cryptocurrency. And reports show an increasingly blurred line between business and government impersonation scams: many scammers impersonate more than one organization in a single scam – for example, a fake Amazon employee might transfer you to a fake bank or even a fake FBI or FTC employee for fake help.[6]

While these scams come in many different forms, the top five described below account for nearly half of 2023 reports.[7]

1. Copycat account security alerts

Topping the list are messages about supposed suspicious activity or unauthorized charges. The message might say it's from Amazon, alerting you that someone's ordered a big-ticket item using your account. Or it might look like it's your bank, asking you to verify a charge. These messages often include a phone number to call or ask you to text back YES or NO. Though scammers are convincing, it's not really Amazon or your bank. It's a scammer who says they can help fix the problem, which is *also* fake. What they tell you to do is really designed to steal your money. Often, this means transferring funds or loading cash into a Bitcoin ATM to "protect" it.

2. Phony subscription renewals

Up next are scams that look like routine email notices that an account you never opened is about to auto-renew to the tune of hundreds of dollars. Often, they say it's an account with Geek Squad.[8] Of course, it's not really Geek Squad; it's a scammer. If you call to sort it out, they'll say they have to connect to your computer to process your "refund." Once in, they make it look like too much money was refunded. They demand that you return the difference, often by buying gift cards and giving them the numbers on the back.

3. Fake giveaways, discounts, or money to claim

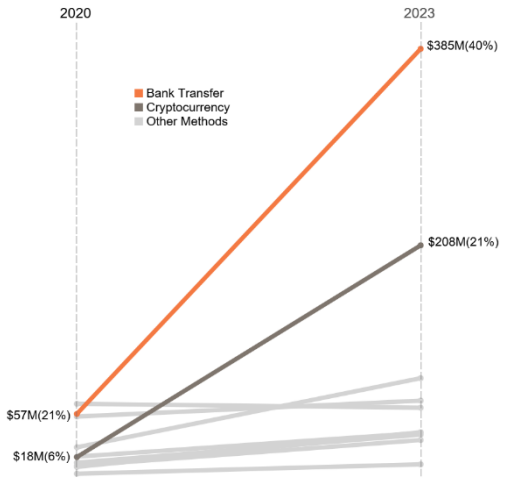
A message about a giveaway, discount, or free money may seem to come from a company you know – say, discounts from your internet provider, a giveaway from a big retailer, or sweepstakes winnings from Publishers Clearing House. Sometimes the so-called offer is about government money you can supposedly claim. These stories are all just another set-up to steal your money. The story ends with you buying gift cards or sending money to claim the deal, gift, or sweepstakes. And that's always a sign of a scam.

4. Bogus problems with the law

Scammers pretending to be government agents say your identity has been used to commit a serious crime – often, they claim, money laundering or drug smuggling. They then offer to help you fix the supposed problem, which always involves them telling you to move money or put it on gift cards. For example, many people reported being told to load cash into Bitcoin ATMs to supposedly protect their funds during a so-called investigation. The scammers even called these ATMs "safety lockers." But this is another scam, and every part of the story is a lie. Money you move is money they steal.

Changing Payment Methods

From 2020-2023, reported dollar losses through bank transfer and cryptocurrency have soared.



Figures are based on reports to the FTC Consumer Sentinel Network classified as business imposter or government imposter. This excludes reports provided by Sentinel data contributors, reports that did not indicate a payment method, and payment methods classified as "other." "Bank transfer" refers to a payment category in Sentinel that includes bank wire transfers and ACH payments. Some consumers also select this option for Zelle payments.

5. Made-up package delivery problems

Messages pretending to be from the U.S. Postal Service, UPS, or FedEx say there's a problem with a delivery. They include a link to a website that looks real – but isn't. Some ask for your bank account details. Others ask you to pay a small "redelivery fee," but if you do, the scammer now has your credit card information. And, reports tell us, these scammers quickly start racking up fraudulent charges.

All these scams have tactics that scammers hope give them an advantage. First, their messages look a lot like the messages real companies send: emails or texts about special deals and security alerts on your accounts. Second, they play on your emotions: if you're worried about a problem or excited about a free gift, it can be harder to spot signs of a scam. Finally, they reframe their demands for money to avoid setting off alarm bells: people who'd never send money to a stranger have emptied their accounts, believing they were "protecting" their funds.

So how can you spot and avoid these scams?

- Never click on links or respond to unexpected messages. If you think a story might be legit, contact the company or agency using a phone number or website you know is real. Don't use the information in the message.

- Don't believe anyone who says you need to buy gift cards, use a Bitcoin ATM, or move money to protect it or fix a problem. Real businesses and government agencies will never do that – and anyone who asks is a scammer.

- Slow down. Scammers want to rush you, so, again: stop and check it out. Before you do anything else, talk with someone you trust. Anyone who's rushing you into paying or giving information is almost certainly a scammer.

Learn more about impersonator scams. To spot and avoid scams – and learn how to recover money if you paid a scammer – visit ftc.gov/scams. Report scams to the FTC at ReportFraud.ftc.gov.

The FTC uses reports from the public to investigate and stop fraud, for consumer education and outreach, and for analyses like this. File your fraud report at ReportFraud.ftc.gov. To explore Sentinel data, visit FTC.gov/exploredata.

1 In 2023, business imposter scams were the most reported fraud subcategory, and government imposter scams were the third most reported. These fraud subcategories also ranked among the top three most reported frauds in 2020, 2021, and 2022. This excludes reports categorized as unspecified.

2 This figure and figures throughout this Spotlight are based on reports directly to the FTC. The combined number of business imposter and government imposter reports by year are as follows: 316K (2020), 529K (2021), 458K (2022), 487K (2023). Some reports are classified as both business imposter and government imposter. Because the vast majority of frauds are not reported to the government, these figures reflect just a small fraction of the public harm. See Anderson, K. B., To Whom Do Victims of Mass-Market Consumer Fraud Complain? at 1 (May 2021), available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3852323 (study showed only 4.8% of people who experienced mass-market consumer fraud complained to a Better Business Bureau or a government entity).

3 Excluding reports classified as unspecified, 48% of reports directly to the FTC in 2023 were classified as business imposter or government imposter or both.

4 The combined reported losses to business imposter and government imposter reports by year are as follows: $310M (2020), $673M (2021), $961M (2022), $1.1B (2023).

5 "Bank transfer" refers to a payment category in Sentinel that includes bank wire transfers and ACH payments. Some consumers also select this option for Zelle payments.

6 Reports about FTC impersonation have increased about five-fold since 2020. See FTC Consumer Alert, *The FTC won't demand money, threaten you, or promise you a prize* (July 2023) *available at* https://consumer.ftc.gov/consumer-alerts/2023/07/ftc-wont-demand-money-threaten-you-or-promise-you-prize

7 The top scam types were identified by hand-coding a random sample of 850 reports filed in 2023 classified as business imposter or government imposter that included a narrative describing the consumer's experience.

8 More people reported impersonation of Geek Squad in 2023 than any other impersonated company. The number of reports about Geek Squad impersonation increased over 100-fold from 2020 to 2023. These scams have contributed heavily to the rise of email as the most reported fraud contact method in 2023. See FTC Consumer Alert, *How to recognize a fake Geek Squad renewal scam* (October 2022) *available at* https://consumer.ftc.gov/consumer-alerts/2022/10/how-recognize-fake-geek-squad-renewal-scam.