May 2024

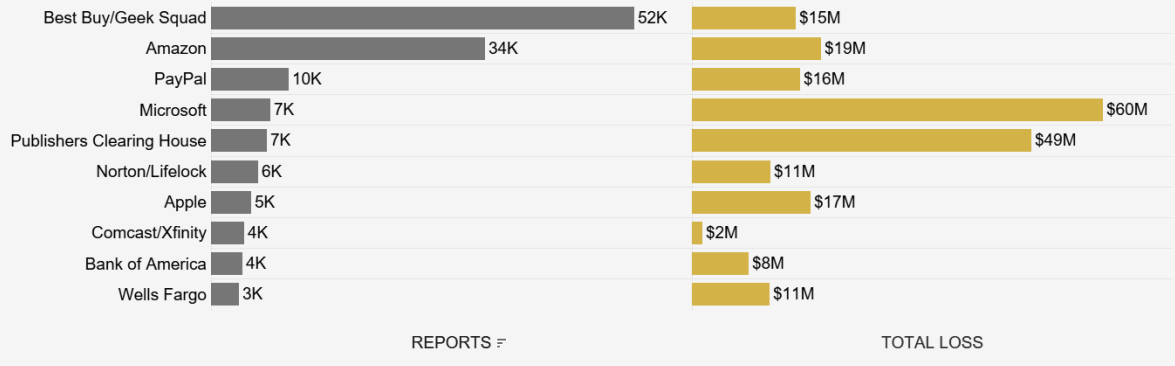
Consumer Protection Data Spotlight
FTC reporting back to you

Who's who in scams: a spring roundup

Scammers are all about spinning lies, but they still operate in the real world. Many scammers pretend to be well-known businesses to gain trust and make their stories seem more believable.[1,2] And scammers use real-world methods to contact people and to get paid. Reports to the FTC's Consumer Sentinel Network point to some of their favorites.

Let's start with the most-impersonated companies. According to 2023 reports, Best Buy's Geek Squad, Amazon, and PayPal top that list. But reported losses tell a different story: losses were highest when scammers impersonated Microsoft and Publishers Clearing House.[3] The scammers impersonating these businesses work in very different ways. For example, phony Geek Squad emails tell you that a computer service you never signed up for is about to renew – to the tune of several hundred dollars. Microsoft impersonation scams start with a fake security pop-up warning on your computer with a number to call for "help."[4] And calls from the fake Publishers Clearing House say you'll have to pay fees to collect your (fake) sweepstakes winnings.

Scammers impersonate some companies more than others. These top ten were the most reported in 2023.



Figures are based on fraud reports to the Consumer Sentinel Network classified as business imposters, tech support scams, and prizes, sweepstakes and lotteries. Reports that do not name an impersonated company and reports provided by Sentinel data contributors are excluded.

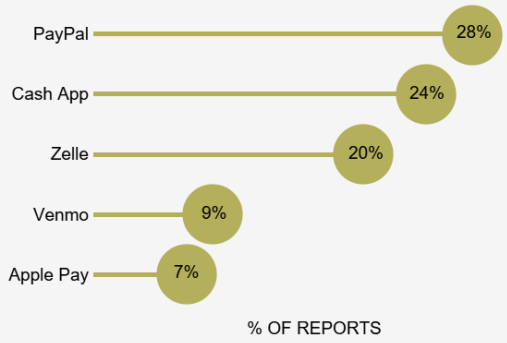
Reports about all types of fraud also tell us how scammers contacted their targets. Last year, people told us that scammers were most often reaching out by email and phone calls. But people also told us that they lost the most money on scams that started on social media.[5] People most frequently named Facebook and Instagram in these reports,[6] and most often reported online shopping scams that started with ads on social media. However, the largest reported losses to scams starting on social media platforms were to investment scams.

How scammers get their money varies by the type of scam, too. For example, people who report investment scams most often say they "invested" with cryptocurrency or via bank transfer.[7] Reported payments to scammers by these two methods added up to the highest losses in 2023, both per person and in total.[8] And many people reported using payment

apps and services, most often in connection with online shopping scams.[9] Most people who reported using a payment app or service named the company they used, with PayPal, Cash App, Zelle, Venmo, and Apple Pay most often reported in 2023.

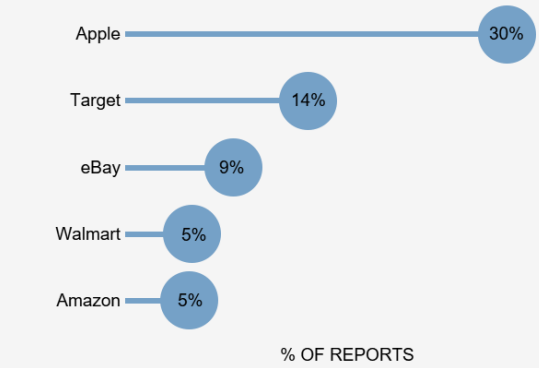
Gift cards were the top reported payment method on several types of scams in 2023, including romance scams, tech support scams, government impersonation scams, and scams that impersonate people you know, like your boss or a grandchild. Reports show that scammers specify what gift card brand to buy, which most people named in their reports. In 2023, Apple cards were far and away the most reported gift card brand, followed by Target, eBay, Walmart and Amazon gift cards.[10]

Nearly 9 out of 10 people who reported paying a scammer with a **payment app or payment service** named one of five top apps or services.



Figures are based on fraud reports to the Consumer Sentinel Network that identified payment app or service as the method of payment. Reports provided by Sentinel data contributors, reports that did not name a payment app or service, and Zelle payments reported as bank transfers are excluded.

Nearly 7 out of 10 people who reported paying a scammer with a **gift card** named one of five top card brands.



Figures are based on fraud reports to the Consumer Sentinel Network that identified gift card or reload card as the payment method. Reports provided by Sentinel data contributors and reports that did not name a card brand are excluded.

So, how can you spot and avoid these and other scams?

- Stop and check it out. Before you do anything else, talk with someone you trust. Anyone who's rushing you into sending money, buying gift cards, or investing in cryptocurrency is almost certainly a scammer.
- Never click on links or respond to unexpected messages, and never trust caller ID. 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 pay anyone who demands that you pay by gift card, cryptocurrency, money transfer, or payment app. Only scammers say there's only one way to pay.

And what can businesses do? At minimum, make it easier for customers to reach you to find out what communications are legit. Of course, shifting responsibility onto your customers isn't the answer, so look to your workforce's ingenuity to deploy solutions that protect your loyal customers and your good name.

To spot and avoid scams – and learn how to recover money if you paid a scammer – visit ftc.gov/scams. Visit business.ftc.gov to get resources and advice for businesses. Report scams to the FTC at ReportFraud.ftc.gov.

1 In 2023, about 332,000 people reported a business impersonation scam, far more than any other fraud type, and reported losses totaled over $660 million. These figures, and figures throughout this Spotlight, exclude reports provided by data contributors. 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).

2 Government agencies, including the FTC, are often impersonated as well. For more information about government impersonation reporting data, including the most reported agencies, see FTC's interactive Tableau Public infographic.

3 Microsoft impersonation reports are generally classified as tech support scams and Publishers Clearing House impersonation reports are generally classified as prizes, sweepstakes, and lotteries. These two Sentinel fraud types were included in this analysis in addition to the business imposter fraud type as they generally include reports about impersonated companies.

4 See FTC Consumer Alert, New tech support scammers want your life savings (March 2024) available at https://consumer.ftc.gov/consumer-alerts/2024/03/new-tech-support-scammers-want-your-life-savings

5 Reported losses to fraud that started on social media by year are as follows: $237M (2020), $729M (2021), $1.1B (2022), $1.4B (2023). More money was reported lost to fraud starting on social media than any other contact method in 2021, 2022, and 2023. For more information about contact method and payment method reporting data, see FTC's interactive Tableau Public dashboard.

6 In 2023, 51% of reports about fraud starting on social media identified Facebook as the social media platform, and 22% identified Instagram. This excludes reports that did not identify a social media platform.

7 Of the $1.8 billion reported lost to investment-related fraud in 2023, $707 million was lost using cryptocurrency and $689 million was lost using bank transfers.

8 In 2023, compared to all other payment methods, total reported losses were highest on bank transfers ($1.7B) followed by cryptocurrency ($1.2B), and median individual reported losses were highest on cryptocurrency ($5,000) followed by bank transfers ($4,581).

9 Credit cards, debit cards, and payment apps and services were the top three most reported payment methods, though people tended to report losing less money to the scammer. In 2023, the median individual reported losses for these payment methods were as follows: payment app or service ($380), credit card ($136), and debit card ($110).

10 For earlier Sentinel data about gift card brands, see FTC Data Spotlight, Scammers prefer gift cards, but not just any card will do (December 2021) available at https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2021/12/scammers-prefer-gift-cards-not-just-any-card-will-do.