Consumer Protection Data Spotlight
FTC reporting back to you

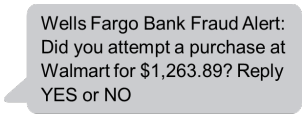
# IYKYK: The top text scams of 2022

Texting is cheap and easy, and scammers are counting on the ding of an incoming text being hard to ignore.[1] In 2022, they were right to the tune of $330 million in losses to text scams, as reported to the FTC's Consumer Sentinel Network, with a median reported loss of $1,000. That's more than double the 2021 reported losses and nearly five times what people reported in 2019.[2] In fact, reports about text scams spiked in the first six months of the COVID-19 pandemic and have never returned to pre-pandemic levels.[3]

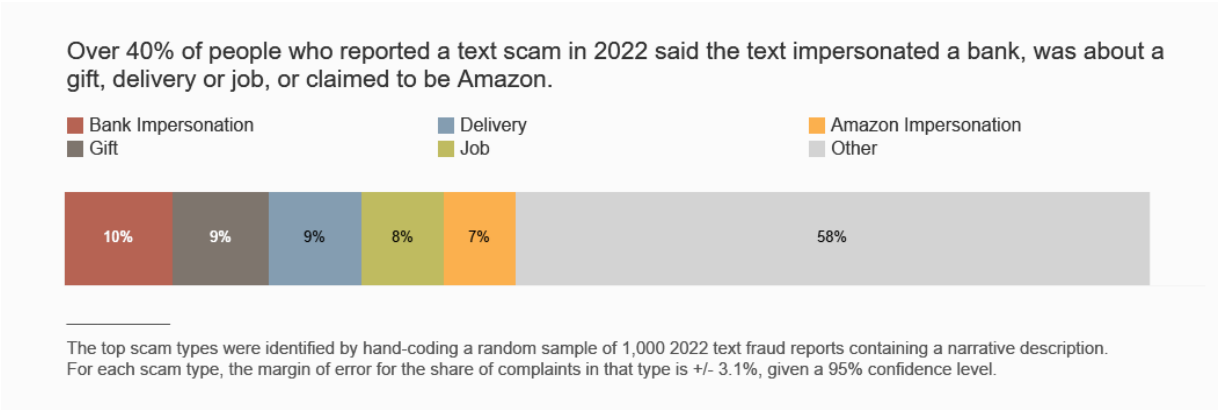
But why do they work? Scammers use the speed of text communication to their advantage: they hope you won't slow down and think over what's in the message. Some messages promise a good thing – a gift, a package, or even a job. Others try to make you panic, thinking someone's in your accounts. These are all lies and ways to take your money and personal information.

While there are countless varieties of text scams, the top five described below account for over 40% of randomly sampled text frauds reported in 2022.[4] All five have one thing in common – they often work by impersonating well-known businesses.[5]

## 1) Copycat bank fraud prevention alerts

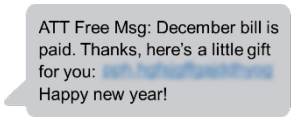



Reports about texts impersonating banks are up nearly twentyfold since 2019.[6] You might get a fake number to call about supposed suspicious activity. Or they might say to reply "yes or no" to verify a large transaction (that you didn't make). If you reply, you'll get a call from the (fake) fraud department. People say they thought the bank was helping them get their money back. Instead, money was transferred *out* of their account. This scam's median reported loss was a whopping $3,000 last year. Worse still, many people report giving their Social Security number and other personal information to scammers, leading to possible identity theft.



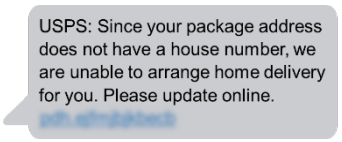
## 2) Bogus "little gifts" that can cost you

A text about a free gift, reward, or prize may look like it came from a company you know – say, your cell phone company or a big retailer. But everything about this is fake. If you click the link and pay a small "shipping fee," you just gave your credit card number to a scammer. Reports tell us fraudulent charges soon follow.



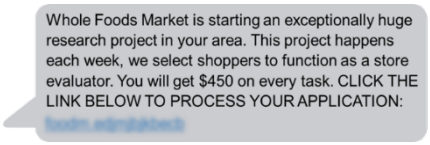

## 3) Fake package delivery problems

Expecting a package? There's a text scam for you. Texts pretending to be from the U.S. Postal Service, FedEx, and UPS say there's a problem with a delivery.[7] They link to a website that looks real – but isn't. If you paid a small "redelivery fee," which many people reported, that was a trick to get your credit card number. People also reported giving these scammers their personal information, including Social Security numbers.



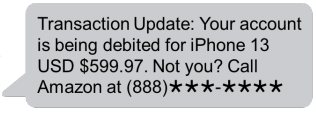

## 4) Phony job offers

Promises of easy money for mystery shopping at well-known stores like Whole Foods and Walmart are an old scammer favorite. Reports about bogus offers to make money driving around with your car wrapped in ads are also common. Reports show job scammers also target people who post their resumes to employment websites like Indeed. In most of these reports, scammers use checks that seem to "clear" but turn out to be fake to trick people into sending them money.[8]




## 5) Not-really-from-Amazon security alerts

Like fake bank texts, texts from someone who says they're "Amazon" look like automated fraud prevention messages. Often, they ask you to verify a big-ticket order you didn't make. If you call the number in the text, you get a phony Amazon rep who offers to "fix" your account. People often report giving the rep remote access to their phone so they can get things fixed and get their refund.[9] But then the rep says a couple of zeros were accidently added to the refund, so they need you to return that money to them – often by buying gift cards and giving the cards' PIN numbers.




In all of these cases, reporting can help stop scam text messages:

- Forward it to 7726 (SPAM). This helps your wireless provider spot and block similar messages.
- Report it on either the Apple iMessages app or Google's Messages app for Android users.
- Report it to the FTC at ReportFraud.ftc.gov.

How can you avoid text scams?

- **Never click on links or respond to unexpected texts.** If you think it might be legit, contact the company using a phone number or website you know is real. Don't use the information in the text message.
- **Filter unwanted texts before they reach you.** There are a few ways to block unwanted texts.

To learn more about how to spot and avoid scams – and how to recover money if you've paid a scammer – visit ftc.gov/scams. Learn more about text scams at ftc.gov/textscams.

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 Text message open rates are estimated to be as high as 98%, and response rates as high as 45%, as compared to email open and response rates of 20% and 6% respectively. More than half of consumers text daily, making texting more common than any other communication method, including voice or email. See FCC, Consumer Advisory Committee, *Report on the State of Text Messaging* at 5 (August 2022), *available at* https://files.fcc.gov/ecfs/download/20970528-9c2e-400d-951b-1024118e50fb?orig=true&pk=cb77b2ec-1a58-dbc6-139b-ad192cfd5d9b.

2 Aggregate reported losses to text fraud by year are as follows: $67M (2019), $86M (2020), $131M (2021), $330M (2022). Text fraud is defined here and throughout this Spotlight as fraud reports indicating text as the contact method. 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 The number of text fraud reports by year are as follows: 137K (2019), 332K (2020), 378K (2021), 330K (2022). The number of reports spiked in Q3 2020, with 125K reports in that quarter alone.

4 The top scam types were identified by hand-coding a random sample of 1,000 2022 text fraud reports containing a narrative description. For each scam type, the margin of error for the share of complaints in that type is +/-3.1%, given a 95% confidence level. The scam types identified here do not replace the subcategories the FTC publishes on www.ftc.gov/exploredata, but rather provide more detail. The subcategories published on www.ftc.gov/exploredata primarily reflect topics consumers self-select on www.reportfraud.ftc.gov or report to the FTC call center or Sentinel data contributors. Reports on www.ftc.gov/exploredata may be tagged with multiple subcategories.

5 In 2022, 51% of reports about text fraud were categorized in Sentinel as business imposters. This excludes reports categorized as unspecified.

6 The number of fraud reports about text messages claiming to be from banks by year are as follows: 1,355 (2019), 2,231 (2020), 13,677 (2021), 25,725 (2022). The top companies identified in 2022 reports about bank impersonation text scams were Bank of America (14%), Wells Fargo (12%), Chase (12%), and Citibank (9%). These figures exclude reports that did not include a company name.

7 Many U.S. Postal Service delivery reports are categorized as government imposters on www.ftc.gov/exploredata.

8 By law, banks must make deposited funds available quickly. The bank may say the check has "cleared" when funds are made available, but it can take weeks for the bank to uncover a fake check. The bank can take back the amount of the check once it is detected as fake. Reports show fake checks are often used to trick people into, for example, sending money to fake car wrap installers or buying gift cards at retailers as supposed mystery shoppers.

9 See the June 2021 Data Spotlight for more information about Amazon impersonation scams.