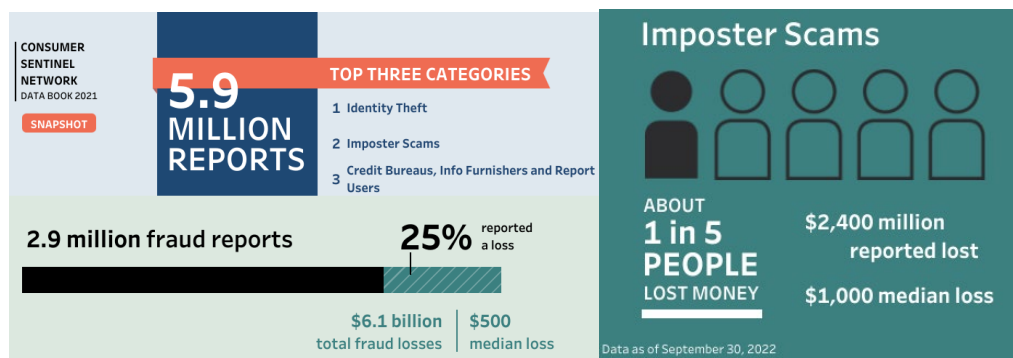


## *Imposter Scams: Detection and Reporting*

Each year the Federal Trade Commission (FTC) releases data about fraud through their Consumer Sentinel<sup>1</sup> Network Data Book. The following infographic represents the top three scams reported to the FTC in 2021. Imposter Scams, which placed number 2 on the list, are the subject of this OPEX Awareness and are increasing in prevalence.



### What are Imposter scams?

An imposter scam occurs when someone pretends to be someone they are not to obtain information or money from you. An imposter scammer may contact you by phone, email, or text claiming to be someone you know, a trusted business, or a government official. Imposters may pretend to be from a wide range of legitimate organizations, including the following:

- Friends or business associates.
- Companies where you commonly do business – your electric company, internet, water, etc.
- Government agencies programs, such as the IRS, Social Security, or Medicare.
- Tech support companies.
- Vacation companies, lotto, or prize associations.
- Charities or other groups that ask for donations.

Imposters may want to steal your money or they may just want you to disclose personal information. Watch for red flags noted below!

Imposters might say:

- ❗ *Hi, I am calling from tech support about a problem on your computer.*
- ❗ *Hello, I am from the IRS and am calling because you owe us back taxes.*
- ❗ *Hi, you won a cruise to a wonderful place! All you have to do is send money to cover the taxes.*
- ❗ *Your friend is in trouble and needs your help! Just send some money right away.*
- ❗ *We accidentally overpaid you, so we need you to send back the extra in the amount of \$XXX.*

<sup>1</sup> Consumer Sentinel is a Federal Trade Commission (FTC) investigative cyber tool that gives members of the Consumer Sentinel Network access to millions of reports about scams, identity theft, and other consumer protection topics to provide greater visibility and support law enforcement efforts.

Imposters might try to get you to pay them by asking you to **buy a gift card** or **wire money**. People who say you **have to pay** that way **are almost always** scammers trying to steal your money! Never send money to people you don't know – or when you are not sure if they are who they say they are. Scammers will typically create a **sense of urgency** around payments. Payments in odd forms such as a gift card and wire transfer are **unusual** for most businesses, and this is a **HUGE red flag** of fraud.

## Real Life Scenarios

*Most people think this can't happen to them, but it can and it does happen to DOE employees all the time. Just this month a co-worker shared this Scam Story<sup>2</sup>:*

*Today I received a text message telling me it was the last day to qualify for 50% off my Xfinity bill. I placed the call to the number that was given to me in the message. It answered with a recording that said I had reached Comcast (Xfinity). The person (Bruce) that I spoke to proceeded to tell me I was eligible for 50% off my Xfinity bill for 3 years, along with some other perks (free premium channels, a free month, etc.). The individual told me "The catch was"... since Target was the sponsoring company for this promotion, I needed to pay 5 months of service in advance (i.e., \$740) via purchasing and using Target gift cards. After that \$740 gift card purchase from a local store, Bruce*



[This Photo](#) by Unknown Author is licensed under [CC BY-SA-NC](#)

*instructed me to then call the "Xfinity Finance Line" at a different 800-number, provide them a six-digit code Bruce gave me, and finally pay for the 50% off promotion by giving the gift card numbers. Then, my February month would be free! Also, if I did this within two-hours, I would receive a two-hundred-dollar visa gift card, too! I almost did this but decided to call Xfinity directly first and ask about this promotion. They proceeded to tell me that this was fraud. Bruce called me 6 times at the two-hour limit, most likely to find out why I did not make this purchase. The first time he called, when I heard it was him, I hung up. I didn't answer any of his calls after the first one. Xfinity is aware of this issue and said they would also look into it.*

Luckily, the DOE co-worker did not make any purchases and spotted this as a scam.

*What were some of the red flags that you noticed in their story? Why might this be concerning?*

- A) There are no red flags in the story. I think this is a real promotion.
- B) Red Flags included: 1) States they are from "Xfinity" but promotion is sponsored by "Target" 2) Needed to pay with gift cards and 3) Created a sense of urgency to complete the task. This is an issue because gift cards are not traceable funds and I will lose my money.
- C) Red Flags included: Paying in advance 5 months with gift cards. This seems odd.

See answer on bottom of page 1.

---

<sup>2</sup> The company names listed in the *Scam Story* are also a victim of fraud and did not participate in any fraudulent activity.

## Reporting and Resources

It is vital that you report any scams that you encounter since this may aid in identifying the source of the scam, trends, and potential areas that affected businesses, agencies, and law enforcement may focus or prioritize during investigations.

If you experience a scam such as an Imposter Scam while performing work for DOE, follow your local processes or procedures such as contacting your local security or counterintelligence office for assistance. For questions on any losses of government funds related to fraud or scams please contact the DOE Office of Inspector General at [ighotline@hq.doe.gov](mailto:ighotline@hq.doe.gov) and for any questions on product related scams or counterfeit items contact [counterfeit@hq.doe.gov](mailto:counterfeit@hq.doe.gov).



[This Photo](#) by Unknown Author is licensed under [CC BY-SA-NC](#)

To learn more about scams such as Imposter Scams, or to report scams that you have encountered at home, go to the FTC website here: [Imposter Scams | Consumer Advice \(ftc.gov\)](https://www.ftc.gov/consumer/advice). Although items found at home are not required to be reported it does aid in trending potential threats and scams by the FTC.