Table of Contents

## Feels off? Log off.

It's easy to believe that you will never fall for a scam. Unfortunately, anyone, regardless of age, background, and technical savvy, can fall for a scam. Scammers utilize social engineering, which uses human psychology against you to steal your money or information. They impersonate your trusted friends and family. They pretend they're law enforcement. They say they love you. They email you a link that downloads spyware on your computer when you click on it. They say they're an employer and ask you to provide your Social Security number as a part of a job application process. They set up cryptocurrencies just to steal investors' money. In short, scammers are everywhere and continually becoming more creative. In 2025, LawNY partnered with <a href="Technically Speaking">Technically Speaking</a> at the Rochester Institute of Technology to launch an educational campaign about fraud and reduce the stigma associated with falling for scams.

In 2023, 2.6 million Americans reported falling victim fraud to the Federal Trade Commission (FTC), with a total of more than \$10 billion lost. Scam-related statistics can be tricky to track because not every victim reports that they've fallen for a scam, meaning that the actual number of people who were scammed and how much money has been lost to fraudsters is likely much higher. Specifically, young adults may not be reporting scams because they're embarrassed, uncertain of how to report a scam, or believe that reporting the scam won't make a difference.

According to the 2023 Better Business Bureau's (BBB) Scam Tracker Risk Report, **35** to **44-year-olds were most likely to be exposed to and lose money from scams**. Although 35- to 44-year-olds were most likely to lose money from a scam

overall, people in different age groups may be more likely to fall for different types of scams.

Certain types of fraud were more prevalent than others among 18-34-year-olds, such online shopping fraud that often starting with social media ads and investment scams, predominantly those involving false cryptocurrency investment opportunities. Younger adults were more than four times more likely to report a loss on an investment (cryptocurrency) scam and more than five times as likely report a loss from a job scam.

It's important to note that people under the age of 20 aren't immune from scammers. Data shows the youngest group of consumers are mainly targeted by scams involving peer-to-peer money transfers and online gaming.

Older adults (those 70 and older) were less likely to report fraud but tended to incur larger financial losses than younger victims. Older adults were more likely to fall prey to tech-support scams and prize, lottery or sweepstakes scams, with a median loss of \$800 for those ages 70-79 and \$1,5000 for those 80 and older.

Reports also point to generational differences in the contact methods that scammers use to reach people. In 2021, 31% of people 18-59 who reported losing money on a scam said it started on a social media platform. For those ages 18-29, it was 40%. In contrast, only 15% of people 60 and over said a scam began on social media.

Not surprisingly, scams starting with phone calls skewed the other way. In 2021, 24% of older adults who reported losing money to a scam said it started with a phone call. Only 10% of younger people who reported losing money to a scam said it started with a phone call.

## Some examples of scams we have seen at LawNY:

- LawNy's Consumer Hotline received a caller from a retired individual who fell for a romance scam. A friend of a friend "introduced" the caller to a person supposedly living in Dubai. After a few years of this "relationship," the caller had sent approximately \$70,000 to the scammer before realizing what was happening. Because the caller had been introduced to the scammer through a person the caller knew in real life, the caller thought the scammer was trustworthy and in love.
- LawNY's Consumer Hotline received a call from someone who had linked their mobile payment app to a social media account. A hacker pretending to be the caller's friend gained access to the caller's social media account and then used the connected mobile payment app to steal the caller's money.
- LawNy's Consumer Hotline received a call from someone whose spouse got a call from a man claiming to be with Microsoft and saying that he could help cancel unwanted Microsoft services. The scammer talked the spouse into allowing the scammer direct access to the spouse's computer. The scammer then used information found on the computer to steal the family's life savings and take out tens of thousands of dollars in credit in the family's name.

The FTC has issued guidance about what to do if you were scammed, which you can read here.

The best way to address fraud and scams is to prevent it from happening in the first place. <u>Click here</u> to read about different types of scams.

If you believe that your personal information has been exposed and your identity stolen, click here.

\* \* \* \* \*

(c) Legal Assistance of Western New York, Inc. ®

This article provides general information about this subject. Laws affecting this subject may have changed since this article was written. For specific legal advice about a problem you are having, get the advice of a lawyer. Receiving this information does not make you a client of our office.

Last Reviewed Date: February 2025

Last updated on February 20, 2025.

Consumer

**Article Legal Information** 

Print

Print

Table of Contents

**NEWS** 

News & publications

More News

August 19, 2025

General Information for Filing an Article 7-D Petition

Can I ask a court to order my landlord to make repairs to my unit? New...

Read More about General Information for Filing an Article 7-D Petition

February 14, 2025

Total and Permanent Disability Discharge for Federal Student Loans

LawNY®'s consumer unit discusses Total and Permanent Disability (TPD)...

Read More about Total and Permanent Disability Discharge for Federal Student Loans

PDF downloaded from https://www.lawny.org/node/618/feels-log