

Guiding Older Adults to Avoid Online Scams

Genevieve Waterman, NCOA
Crystal Thomas, Zelle®
Soo-Lynn Getz, Zelle®

July 13, 2023



Agenda

1. Scams Basics

2. Digital Landscape and P2P Scams

3. Educating and Empowering Older Clients

4. Reporting Resources

5. Questions

Scams Basics



Scams in 2022

1. 2.4 million fraud reports to FTC
2. \$8.8 billion in consumer losses
3. Most losses were through bank transfers (\$1.5 billion) and cryptocurrency (\$1.4 billion).
3. Young adults (age 20-29) reported more losses. Older adults (age 70-79) lost the highest amount of money compared to other age groups.



Scams in 2023 (Q1)

FTC CONSUMER SENTINEL NETWORK

Published April 25, 2023
(data as of March 31, 2023)

Reported Frauds and Losses by Age

Year: 2023 YTD

Year: 2023 Quarter: 1



Text Message Scams

Text message scams accounted for \$330 million in consumer losses in 2022.

Top 5 Text Message Scams in 2022

- Copycat bank fraud prevention alerts
- Bogus “little gifts”
- Fake package delivery problems
- Phony job offers
- Not-really-from-Amazon security alerts

ATT Free Msg: December bill is paid. Thanks, here's a little gift for you: [http://att.com](#)
Happy new year!

USPS: Since your package address does not have a house number, we are unable to arrange home delivery for you. Please update online.
[http://usps.com](#)

Wells Fargo Bank Fraud Alert: Did you attempt a purchase at Walmart for \$1,263.89? Reply YES or NO

Our Speakers

Crystal Thomas



VP of Brand & Marketing at
Zelle®

Soo-Lynn Getz



Director of Fraud Prevention at
Zelle®

Digital Landscape and P2P Scams



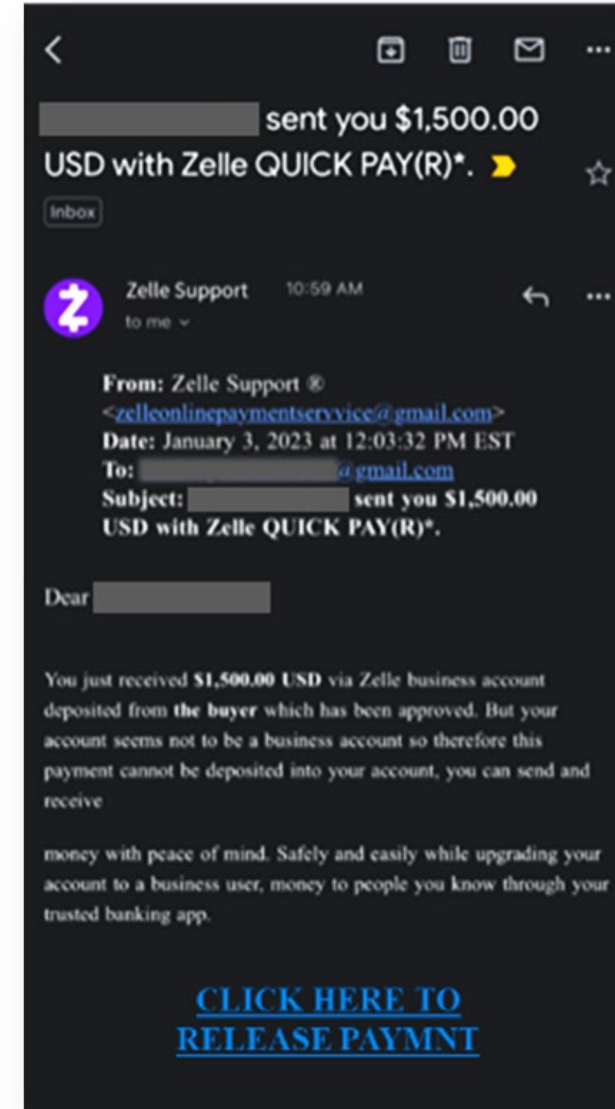
Imposter Scams

Imposter scams are any type of scam where a fraudster attempts to trick you into providing your personal information or sending money.

In 2022, imposter scams were associated with the second highest reported loss amount: \$2.6 billion.

Imposter scams lean on two main methods of luring victims:

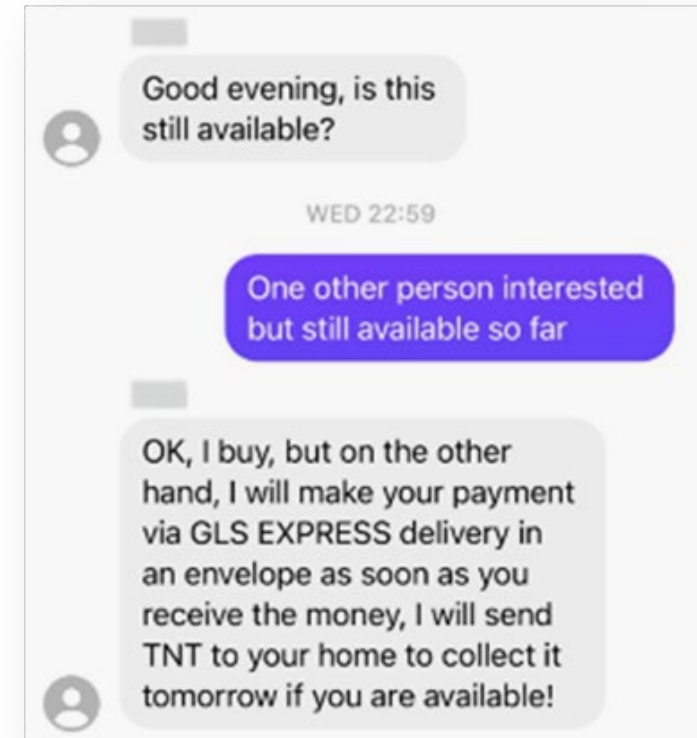
1. Authority
2. Familiarity



Online Marketplace Scams

Both buyers and sellers can fall victim to scams in an online marketplace. Some red flags include:

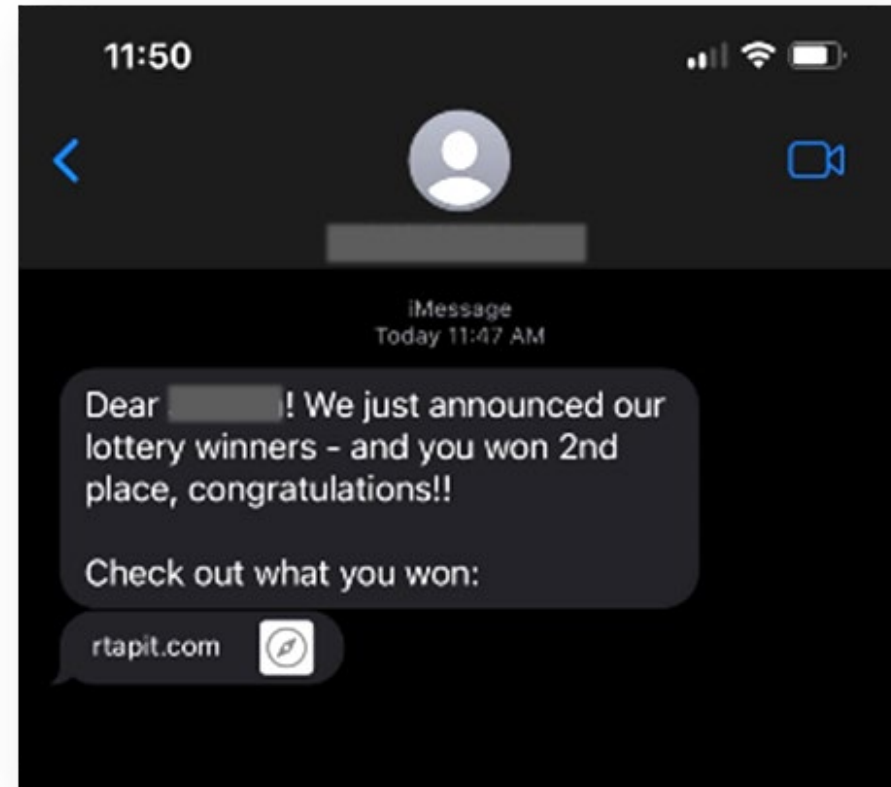
1. Offer may seem too good to be true
2. Product listings that demand specific payment methods
3. False sense of urgency
4. Being asked for one-time passcode
5. Being told to click on links to enter credentials and/or change passwords
6. Being forced to use specific nonpayment protection payment methods



Prize Sweepstakes Scam

Scammers may impersonate well-known sweepstakes organizations to build trust among their victims.

Scammers will send a check, and then request a digital payment to cover taxes, shipping and handling, or processing fees. Legitimate sweepstakes do not work this way.



Educating and Empowering Older Clients



Tips for Safely Navigating Digital Landscape

1

Check Email Domains

2

Don't Trust Caller ID

3

Beware of Fake Links

4

Never Give Out One-Time Passcodes

5

Research the Company

6

Check for Spelling Errors

Tips to Stop Scammers in their Tracks

Use Official Contact Info

Confirm the company/agency trying to reach you is legitimate by contacting the phone number or email listed on their official website.

Forward Scam Texts to 7726

Copy the message and forward it to 7726 (SPAM) before deleting the text.

Check for Filtering Options

Wireless providers might have a tool or service that lets you block calls and text messages.

Check your device's settings to filter messages.

Do a Quick Search

Search online for the name of the company and words like "review," "scam," or "complaint."

Reporting Resources



Reporting Scams

If you think you've been a victim of a scam, use the following resources to report the crime:

- Report the scam to your bank, credit union, or credit card company
- Contact your local authorities
- Report it to the FTC: reportfraud.ftc.gov
- National Elder Fraud Hotline: 833-FRAUD-11

Questions

