FGB FINANCIAL FOUNDATIONS
• Financial Education for Everyone •

IDENTITY THEFT

"TRUST, BUT VERIFY."
- RONALD REAGAN

<u>IDENTITY THEFT</u> happens when someone steals your personal information (name, social security number, bank account number, etc.). The goal is to use your personal information to drain your bank accounts, open and use credit cards in your name, and more!

> *About 86% of people worldwide become the victim of identity theft at least once in their lifetime.*

"The police can't protect consumers. **People need to be more aware and educated about identity theft.** *You need to be a little wiser, a little bit smarter, and there's nothing wrong with being skeptical. We live in a time where if you make it easy for someone to steal from you, someone will."* - Frank W. Abagnale

FIRST GUARANTY BANK Member FDIC

COMMON TYPES OF SCAMS

Protect yourself against fraudsters and their schemes by knowing the signs and what to look for when it comes to common scams.

1. PHISHING

- Urgent emails or texts that look legit but are usually slightly off in the details and punctuation/grammar. Scammers use these to try to get bank account information, log in credentials, and other personal information.

2. RANSOMWARE

- Ransomware is software that holds your device hostage by restricting access until you pay. It is spread to your devices when you click on an infected email attachment or link.

3. IMPOSTER FRAUD

- Imposters solicit you for money by impersonating authorities like the IRS and local police.

4. ELDER FRAUD

- Scammers attempt to sound like grandchildren or family members in trouble to get money from the elderly.

5. ROMANCE SCAMS

- Scammers pretend to fall in love with people to win their trust and steal their money. These types of scams are often initiated on dating sites and social media platforms.

6. EMPLOYMENT SCAMS

- Scammers may pose online as employers or recruiters and ask you to deposit an official-looking paycheck into your account and wire a portion of it to someone else.

7. PEER TO PEER PAYMENTS

- Scammers will use platforms like Zelle, Venmo, and Paypal to trick you into sending money for goods and services that never arrive.

Notes:

DATA BREACHES

The number of people affected by data breaches in the first half of 2024 totaled more than 1 billion. Research released July 2024 by the Identity Theft Resource Center, said “1,571 breaches were reported during the first six-months of 2024, impacting 1.07 bililon victims.”

TOP 5 DATA BREACHES

1. YAHOO - 3 BILLION USER ACCOUNTS EXPOSED
2. MICROSOFT - 30,000 US COMPANIES | 60,000 WORLDWIDE
3. REAL ESTATE WEALTH NETWORK - 1.5 BILLION RECORDS BREACHED
4. FIRST AMERICAN FINANCIAL CORP - 885 MILLION RECORDS LEAKED
5. FACEBOOK - 530 MILLION USERS EXPOSED APRIL 2021

IDENTITY THEFT FACTS

- On average, yearly 14.5 billion Americans become victims.
- Every **39 seconds**, there’s a cyber-attack somewhere in the world.
- A ransomware attack happens every **14 seconds** globally.
- Ransomware crimes jumped by 102% in early 2021.
- 300,000 Americans become victims of phishing every year.
- 1.3 million children’s records are stolen every year.
- 94% of malware is delivered by email.
- 40% of Americans believe their personal information is at risk using public Wi-Fi.
- 50% of ID Theft attacks are more likely to happen after shopping online.
- 87% of people unknowingly provide personal information on the internet.
- 26% of identity theft victims are likely to be repeat victims.
- It takes an average of 30 days to discover a fraudlent account.
- Stolen SS#s, dates of birth, and names are likely to be sold on the dark web for $60-$80.
- Stolen credit card data can be sold on the dark web for as little as $0.50 per card.
- 64% of Americans have not checked to see if they have been affected by data breaches.
- Over 60% of Americans did not have any insurance when identity theft happened.
- Over 84% of teens and young adults fall prey to shopping scams.
- Indentity theft and fraud cost Americans $43 billion in 2023
- Every **22 seconds** there is an identity theft case.
- It takes an average of 6 months and 200 hours to recover from identity theft.

PUBLIC WIFI SCAMS

Hackers may exploit security flaws on a public WiFi router and scan data that passes back and forth between the individual's computer, tablet, or phone. **Example:** a user logs onto a banking website or shops online while on a public network. Personal or financial information could be at risk of exposure.

- **How to Protect Yourself:** Don't log in to banking or other sensitive sites while on public Wi-Fi networks and don't visit sites that require you to enter your password.

BLACKMAIL - INVASION OF PRIVACY

With smartphones everywhere, someone could be captured on video or photographed without their knowledge or consent. In some cases, those images may fall into the wrong hands.

PHONE SCAMS

You sould never give unsolicited callers personal information. **Example:** The Louisiana State Police would NEVER ask for any type of personal identification, payment, or monetary donation over th phone.

15 AMAZON SCAMS TO AVOID

1. Sellers Asking for Payments Off-Platform
2. Call Requesting Personal Information
3. "Mystery Boxes"
4. You're Owed a Refund
5. Text Messages Claiming to be From Amazon
6. Fake Listings with Real Reviews
7. Amazon Prime Video Scam Websites
8. Demanding Payment with Amazon Gift Cards
9. Lookalike Amazon Pages
10. Fake Invoices for Purchases
11. Technical Support Scams
12. Phishing Emails
13. Packages You Didn't Order
14. Fake Job Offers
15. "Write a Review" Scams

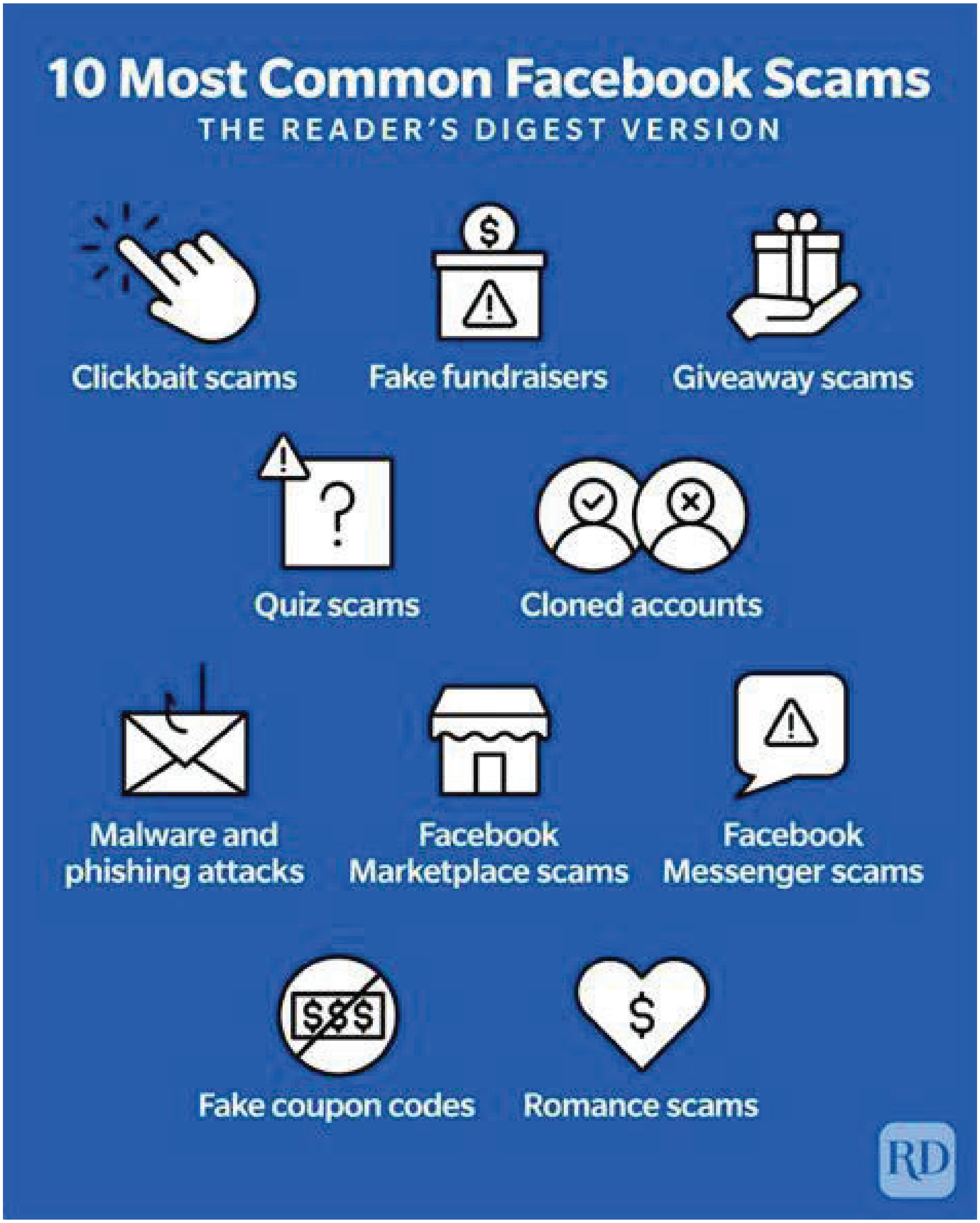
14 VENMO SCAMS TO AVOID

1. "Mistake"Money Transfers
2. Fake Friends Asking for Help
3. Scammers Selling Hard-to-Find Items
4. Fake Payment Invoices
5. Overpayment from Online Purchases
6. Fake Emails or Texts
7. Strangers Who Ask to Use Your Phone
8. "Money Circle" Investment Scams
9. Fake Prizes and Rewards
10. Scammers Posing as Venmo Support Agents
11. Fake Venmo Websites
12. Job Scams
13. Sending Fake Checks
14. Romance Scammers Asking for "Gifts"

ZELLE SCAMS TO AVOID

1. Money Mule Scams
2. Zelle Transfers "to Yourself"
3. Account Upgrade Scams
4. Bank Impersonators
5. Account Takeovers

Notes:



RD.com

NOTE: Facebook has approximately 553 million users from 106 countries with over 32 million users in the US, 11 million in the UK, and 6 million in India. If you are active on social media, you are **30-46%** more likely to be at risk of identity theft and/or account takeovers.

Notes:

DID YOU KNOW
Voice cloning AI Scams are on the Rise

The growth of AI (artificial intelligence) has made it easier for criminlas to clone voices and make messages that sound like people you know. According to the Federal Trade Commission reports from 2022, the US lost $2.6 million to imposter scams.

SCAMS AND YOUR IPHONE

STOLEN IPHONES

What do people do with stolen iphones? First, they attempt to phish it on their own. If they have your name and contact info, they can send a text, email, or voice message to you, pretending to be Apple.

Theives can also break the SIM card out of your phone, put it in a new iPhone, find your email address, and try to get into your iCloud account. If they have your iCloud keychain information, they also have any passwords you've stored there. They can then reset the phone to factory settings and sell it.

What should you do if your iPhone is lost or stolen? Try locating it with the "**Find My**" **app** on iCloud. If you've enabled "**Find My iPhone**" and activate lost mode, it may be easier to locate on a map. If your phone has been stolen or lost, you should also report it to the authorities and your cell service provider.

Notes:

IF YOU THINK YOU'VE BEEN A VICTIM OF IDENTITY THEFT, HERE'S WHAT TO DO

- Contact the three major credit reporting agencies and ask them to <u>**place fraud alerts and a credit freeze on your accounts.**</u> They will share it with the other reporting agencies.
  - **Equifax** - Information Services LLC - P.O Box 740256 Atlanta, GA 30348
    Phone Number: 866-349-5191
  - **Experian** -- P.O Box 4500 Allen, TX 75013
    Phone Number: 888-397-3742
  - **Transunion** -- P.O Box 2000 Chester, PA 19016
    Phone Number: 800-916-8800

According to the FTC, more than $5.8 billion is lost due to fraud each year

- Contact **The Federal Trade Commission (FTC)** online at IdentityTheft.gov or call **(877) 438-4338**.
- Contact the fraud department at our bank/other institutions where you have accounts.

NOTE: If you are a victim of fraud or identity theft, you have the right to request (the credit reporting company) to block the information from your credit report that was the result of identity theft, dispute information you believe is incorrect, and request a fraud alert be placed on your credit report.

WHAT IS A FRAUD ALERT?

A fraud alert is used to inform creditors that you may be a victim of fraud or identity theft. A fraud alert can make it more difficult for a thief to open accounts in your name. **The fraud alert requires creditors to verify that you are the person adding new credit accounts/changing limits** by contacting you via a phone number that you provide.

- There are three types of alerts you can place on your file:
  - **Initial Fraud Alert** - If you suspect that you have been or are about to become a victim of fraud or identity theft (duration: one year)
  - **Extended Fraud Alert** - If you are a victim of fraud or identity theft; requires a copy of the identity theft report (duration: seven years)
  - **Active duty military alert** - If you are in the military and want to minimize your risk of fraud or identity theft while you are deployed (duration: one year)
- NOTE: Placing a fraud alert does not affect your credit. However, it may slow down the approval process for new credit.

WHAT IS A SECURITY FREEZE?

A security freeze prevents unauthorized credit, loans, and services in your name. You must request a freeze with each of the three credit reporting companies. With a freeze, **businesses can't access your credit report for new applications.** Before applying for new credit, you'll need to temporarily lift the freeze according to the credit reporting company's procedures.

HOW TO PLACE OR LIFT A CREDIT FREEZE

- Freeze or lift the freeze on your credit report for FREE by contacting each of the three major credit reporting agencies:
  - **Equifax**
  - **Experian**
  - **TransUnion**

  You can submit your request online, by phone, or by mail.

HOW LONG DO FREEZE REQUESTS TAKE?

- Freeze requests:
  - Online or by phone: agencies must freeze your credit report within one business day
  - By mail: agencies must freeze your credit report within three business days
- Unfreeze requests:
  - Online or by phone: agencies must lift the freeze within one hour
  - By mail: agencies must lift the freeze within three business days

OTHER STEPS YOU CAN TAKE

- Contact the security or fraud departments of each business where an account was opened or charged without your knowledge.
- Follow up **in writing**, with copies of supporting documents.
- Keep copies of documents and records of your conversations about the theft.
- Complete an **ID Theft Affidavit** and include it with your written statement.
- File a report with law enforcement officials and provide copies to all creditors needing proof of the crime.
- Report to the creditor the accounts that you know, or believe, have been tampered with or opened fraud-ulently.
- Report identity theft to the “Consumer Financial Protection Bureau” by submitting a complaint. Your complaint helps law enforcement officials across the country in their investigations. Visit the CFPB's website to find out more information on submitting an identity theft complaint.
- Get a free personal recovery plan that walks you through each recovery step, pre-fills letters/forms for you to send, and tracks your progress on **IdentityTheft.gov.**
- If you get an IRS notice in the mail that says someone used your Social Security Number to get a tax refund, follow the instructions in the letter and fill out an IRS Identity Theft Affidavit (Form 14093).

FEDERAL TRADE COMMISSION
IdentityTheft.gov

TIPS TO AVOID IDENTITY THEFT

CREATE STRONGER PASSWORDS + CHANGE THEM OFTEN

- Be creative with your passwords – stay away from obvious passwords like your zip code, year of birth or sensitive information such as your mother's maiden name or your social security number. Change your passwords every 30 to 60 days. Use a mix of letters, numbers, and symbols and try to use longer phrases instead of single words, such as:

Mary3hadalittleL@mb!

CHECK BANK STATEMENTS AND CREDIT REPORTS

- Regularly review your bank statements for unauthorized transactions and check your credit report for fraud. If you receive paper statements, be sure to shred them.

UTILIZE CYBERSECURITY/ANTI-VIRUS SOFTWARE

- Secure your electronic devices with antivirus and security software. By keeping anti-virus and anti-spam software up to date on your computer, you make it more difficult for scammers to access your personal and account information.

TYPE, DO NOT CLICK

- If you accidentally open a suspicious email, don't click on any links. Even if you think the email is legitimate, type web addresses into your browser instead of clicking on links.

LIMIT SHARING ON SOCIAL PLATFORMS

- Limit your personal information on social media sites, especially if you use the data for passwords or security questions.

LOOK BEYOND THE LOGO

- To make fraudulent emails or web sites appear real, scammers often include actual logos and images of legitimate companies.

SECURE YOUR NETWORK

- Avoid accessing sensitive data on public Wi-Fi networks. Use private browsers, VPNs, and privacy-focused search engines to help prevent identity theft.

Notes:

DESTROY FINANCIAL STATEMENTS

- Don’t throw bank statements, credit card or utitlity bills, or other papers that include personal information in the trash. Invest in a high quality document shredder.

BE AWARE AT ATMS

- Always be aware of your surroundings when entering your PIN at the ATM.

DON’T RESPOND TO CALLS, TEXTS, OR EMAILS FROM UNKNOWN SOURCES

- Additionally, never share personal information via the phone, email, or text. Guard your information closely.

PROTECT YOUR SOCIAL SECURITY NUMBER

- If someone asks for your SSN, ask them why they need it, how it will be used, and how they will protect it. NOTE: You can refuse to disclose your SSN, but the requester can also refuse services if you do not give it.

HOLIDAY SCAMS

Scams are known to increase during the holidays and experts recommend several steps to help protect you and your loved ones from cyber heists so you can enjoy the season. Stay vigilant!

- **Strengthen Passwords and Authentication**
  - Use strong, unique passwords and consider going passwordless. Avoid reusing passwords and enable multi-factor authentication and consider using password managers or authentication apps.
- **Secure Your Connection**
  - Avoid making purchases on public Wi-Fi. Use a VPN to encrypt your connections and protect your personal data.
- **Verify Website Security**
  - Shop only on websites with "https://" and a padlock icon. Be cautious of spelling errors and use official retailer apps or direct links.
- **Beware of Phishing Emails**
  - Check the sender's email domain and look for typos. Avoid clicking on suspicious links.
- **Avoid Malicious Browser Plug-ins**
  - Use anti-malware software and secure browsers like DuckDuckGo to protect your payment information.
- **Watch Out for Fake Online Stores**
  - Be cautious of new, unfamiliar storefronts with unbelievably low prices, especially during Black Friday and Cyber Monday. Verify the authenticity of website linked on social media.
- **Be Cautious with Donation Sites.**
  - Verify the legitimacy of donation sites to avoid scams.

Notes: