Identity Theft & Fraud Prevention Workshop

AKAMAI INVESTMENT ADVISORS
Financial Planning & Portfolio Management

PRESENTED BY:

JAMIE HANSON

INVESTMENT ADVISOR REPRESENTATIVE

608.729.3874
2960 Triverton Pike Dr. Suite 100 Fitchburg WI 53711

1

BACKGROUND

- Originally from Appleton, attended & graduated from UW Madison
- Co-founder & Partner Akamai Investment Advisors
- Certified Financial Fiduciary
- Behavioral Financial Advisor Designation (BFA)
- Member Benefit Partner of the Wisconsin Retired Educator's Association (WREA)

WREA

2

The Crime Of The 21st Century

- Financial Fraud is one of the most common yet under-reported forms of elder abuse
- The Federal Trade Commission (FTC) reports 48% of Fraud Complaints & 19% of Identity Theft complaints impacted Seniors in 2023
  - As the population of Seniors increases, so does the number of people willing to take advantage of them
- People age 65+ lose a whopping $28.3 billion to elder financial abuse each year

Source: FTC & AARP 2023 Study

3

Is Fraud the same thing as Identity Theft?

- No, they are not the same even though they are often used interchangeably
- Fraud: the act of stealing and misusing personal information and existing accounts of a victim
- Identity Theft: the act of taking stolen information to open and abuse new accounts under the victim's name

  - Example: Data breach and your personal information was stolen.
    - Hacker makes unauthorized purchases on an existing credit card (Fraud)
    - Hacker takes the information and applies for benefits or opens new credit cards in your name (ID Theft)

Source: TrueLink 2023Study

4

Fraud or Identity Theft: 2 BIG Differences

The damages involved and the liability

If you are a victim of credit card fraud, someone is using your card without permission and adding charges fraudulently. In this case, the card company will block the card and notify you. As far as liability goes, whatever the thief buys, the maximum you'll have to pay will be $50. In most cases you won't even have to pay that.

Identity theft is much more severe. Someone is pretending to be you, applying for cards, driver's license, phones etc. You may be liable for all that activity since it is not as easy to prove what was the "real you".

Tip: Identity Theft cannot happen without fraud, however, fraud CAN happen without it leading to Identity Theft.

Source: TrueLink 2023 Study

5

3 General Categories Of Fraud

- Employee Fraud: Embezzling, Selling Trade Secrets
- Government Fraud: Insurance, Tax, Medicare & Social Security fraud
- Consumer Fraud: Telemarketing scams, Grandparent scams, Credit Card, and Identity Theft

Source: TrueLink 2023 Study

6

2.4 million complaints to the FTC were fraud related

Rank	Consumer State	Complaint Reports per 100,000 population	Complaint Reports
1	Georgia	1,550	162,957
2	Delaware	1,506	14,570
3	Nevada	1,455	44,081
4	Florida	1,446	306,735
5	Maryland	1,363	82,287
39	Wisconsin	760	44,120

Source: FTC Consumer Sentinel Network Data Book 2022

7

Most Common Fraud Schemes/Scams

Telemarketing Fraud

- One of the most common schemes
- Usually, cold calls or direct mail
- High Pressure Tactics: Act NOW, Can't afford to miss this "no risk" offer
- Once deal is made victim's name is put on a "suckers list" & shared with other scam artists

Examples:

- Caller says they are with your bank or credit card company, and they need to verify information
- You have won a "free gift" BUT you must pay postage and handling
- Cross-Border Fraud: "guaranteed" to have won a vacation, car or money BUT the winner must pay fees for shipping, taxes, customs, insurance etc.

Tips for avoiding Telemarketing Fraud

- Put your phone number on the "Do Not Call" Registry **www.DoNotCall.gov**
- Ask for the offer to be put in writing
- Never agree to wire money or give out credit card/bank account information

Source: National Crime Prevention Council

8

Most Common Fraud Schemes/Scams

Grandparent Scam

- Scam artists contact unsuspecting grandparent by phone
- May pose as law enforcement, medical personnel or the "grandchild"
- Scammer states there has been an arrest or injury or some other emergency, often outside of the U.S.
- Most Grandparents are extremely alarmed and will doing anything to help their grandchild

Tips for avoiding Grandparent Scams

- Be wary of unsolicited contacts to wire money
- Don't fill in the blanks- "It's your grandson" say "which one?"
- Contact the family member directly or immediate relatives to confirm the story
- Never provide bank or credit card information to any caller for any reason

Source: National Crime Prevention Council

9

Most Common Fraud Schemes/Scams

Credit Card Fraud

- The most prevalent type of fraud
- Over 65% of Americans have complained about credit card fraud
- Popularity of online shopping makes "Card Not Present" fraud 81% higher than Point-of-Sale fraud

- Holiday shopping season is a high time for fraud attempts
  - 1 out of every 85 transactions is a fraudulent attempt
  - Thanksgiving Weekend, Dec 11-16th & Christmas Eve

Tips for avoiding Credit Card Fraud

- Avoid using public WI-FI for banking or purchases
- Don't share your personal financial information over the phone or email
- Create strong passwords and change them often
- Scrutinize your monthly credit card statements

Source: National Crime Prevention Council

10

Most Common Fraud Schemes/Scams

Identity Theft

- The theft of an individual's Personal Identifiable Information and subsequent use of their identity to create new accounts using all, or portions of, their information. This includes using a stolen Social Security number to open a credit card in someone else's name

- Thieves will create fake addresses for tax notifications, court summons, medical bills and other documents connected with the identity crimes they have committed to keep you in the dark for as long as they can.

Let's take a closer look at the types of identity theft that can occur

SOURCE: NATIONAL CRIME PREVENTION COUNCIL

11

According to the FTC, these crimes falls into 6 major categories

1. Employment- or tax-related fraud (34%)
What it is: A criminal uses someone else's Social Security number and other personal information to gain employment or to file an income tax return.

2. Credit card fraud (28%)
What it is: The thief uses someone else's personal information to open a new credit card account.

3. Phone or utilities fraud (13%)
What it is: The criminal uses another person's personal information to open a wireless phone or utility account.

4. Bank fraud (12%)
What it is: The fraudster uses someone else's personal information to take over an existing financial account or to open a new account in someone else's name.

5. Loan or lease fraud (7%)
What it is: A borrower or a lessee uses someone else's information to obtain the loan or lease.

6. Government documents or benefits fraud (7%)
What it is: The criminal uses stolen personal information to obtain government benefits.

Source: www.ftc.gov

12

Identity Theft Complaint Report by State

Rank	Victim State	Complaints per 100,000	Complaint Reports
1	Georgia	574	60,348
2	Louisiana	534	24,898
3	Florida	524	111,221
4	Delaware	484	4,682
5	Texas	397	113,808
36	Wisconsin	143	8,319

Source: FTC Consumer Sentinel Network Data Book 2022

13

Identity Theft is skyrocketing

- Nearly 60 million Americans have been affected by identity theft, according to a 2022 online survey by The Harris Poll
- In 2023, the Identity Theft Resource Center (ITRC) counted a new record high of 3,205 data breaches, exposing more than 353 million records

- **The Big One= Equifax**
- 147.9 million potential victims
- Breached information: names, social security numbers, birthdates, addresses, driver's license numbers
- #1 Largest Data Breach in last 10 years?

Yahoo! Over 3 billion accounts exposed

Source: www.ftc.gov

14

Why Is ID Theft on the Rise?

- Computers have made record keeping faster. Automation also removes human analysis, making it easier for someone to steal an identity or pose as another person
- Our society is more mobile than ever. Electronic transactions continue to increase dramatically
- Identity Theft is extremely profitable.
  - Hackers now go for monetary returns, not for the thrill of conquering another computer

Source: www.consumeraffairs.com

15

Who Is Vulnerable?

People who:

- Keep money in bank accounts
- Use credit or debit cards
- Generate trash with unshredded paper in it
- Casually toss credit card or other receipts into public receptacles
- Get personal bills by mail or electronically
- Don't check their credit card and bank statements regularly
- Don't check their credit bureau reports regularly
- Have unlocked, easily accessible mailboxes

EVERYONE IS VULNERABLE

SOURCE: NATIONAL CRIME PREVENTION COUNCIL

16

How is an Identity Stolen?

- From your trash in the dumpster
- From your wallet, purse or mailbox
- Obtaining your credit report
- Skimming: duplicating your credit card
- Shoulder surfing
- Hacking and/or data breach
- Telephone calls asking you to "update your records"
- Phishing

www.lifelock.com

17

What is Phishing?

The general term to describe an attempt to acquire personal information such as usernames, passwords or financial information via impersonation or by spoofing.

- Pharming
- Vishing
- Smishing
- Phishing

www.consumer.ftc.gov

18

Pharming

- a fraudster installs malicious code on a personal computer or server.

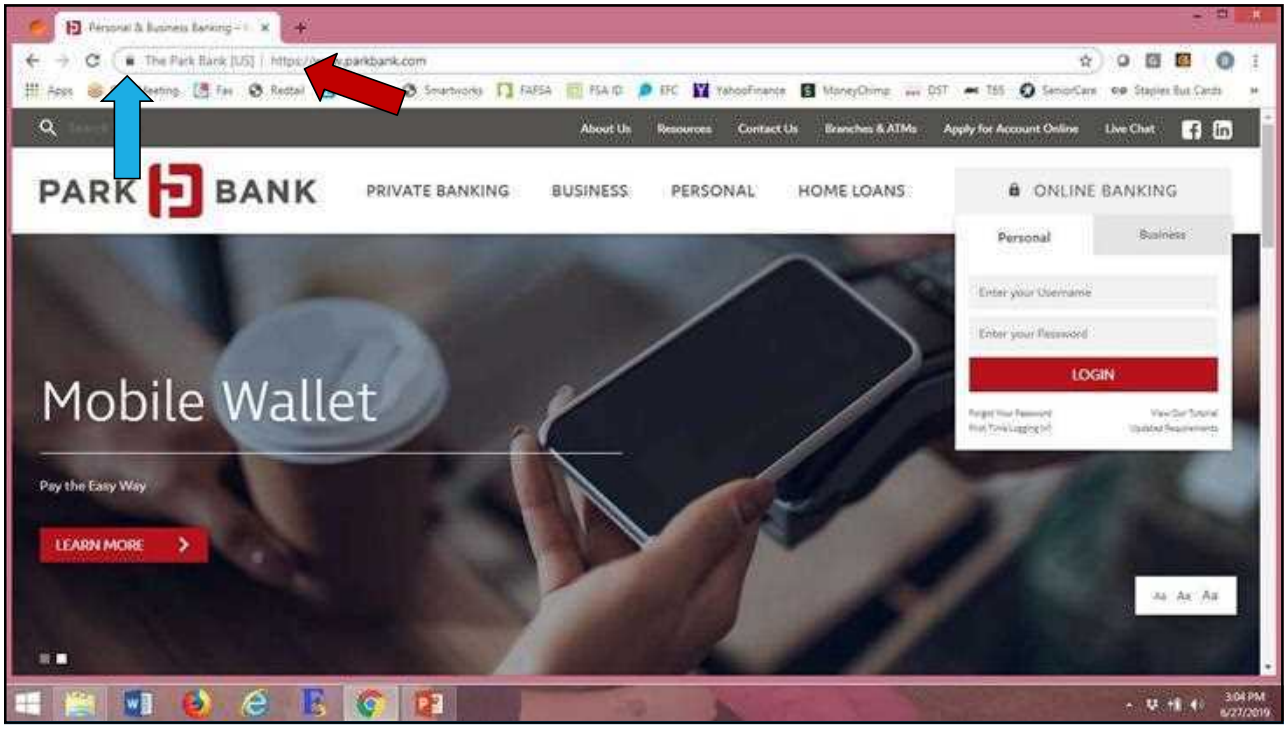
The code tells the computer to redirect any clicks to a fraudulent website without your consent or knowledge

Tips:

- **Look for the "s" in https and the key or lock symbol at the bottom of the browser.**
- **If the website looks different than when you last visited (spelling errors etc.) then don't click on anything unless you are absolutely sure it's a secure site.**

Source: www.ftc.gov

19



20

Vishing

- Fraudsters also go "old school" and use the telephone to obtain your personal information.
- Vishing relies on "social engineering" techniques to trick you into providing info that others can use to access your important accounts or to assume your identity and open new accounts

To avoid being fooled by a vishing attempt:

- If you receive an email or phone call requesting you call them back look up the organization's customer service number to see if it matches the one in the solicitation email or phone call
- Forward the solicitation email to the customer service or security email address of the organization and ask them if the email is legitimate

Smishing

- Uses cell phone text message to lure consumers in
  - The text will often contain an URL or phone number
  - In many cases, the smishing message will be from a "5000" number instead of an actual phone number

Tip: Do not respond to any smishing message

Source: www.ftc.gov

21

Phishing

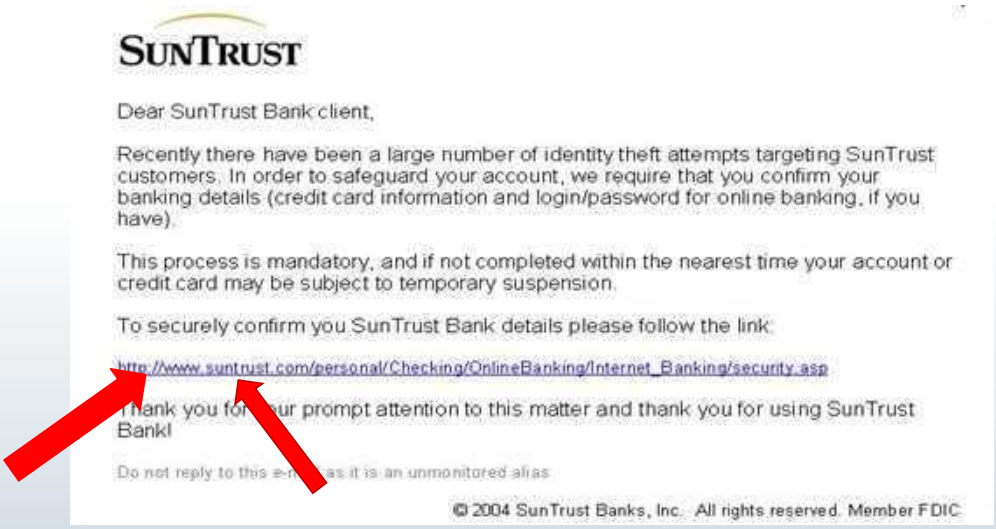
The most common method of online identity theft and virus spreading using platforms such as social media or email to acquire personal information, including login credentials or account information

- Emails continue to be the major source of phising scams however social media attacks have climbed from 8.3% to 84.5% in just seven years
- Criminals often masquerade as reputable entities such as banks, utility and credit card companies

NATIONAL CRIME PREVENTION COUNCIL

22

Example of Phishing Email



SUNTRUST

Dear SunTrust Bank client,

Recently there have been a large number of identity theft attempts targeting SunTrust customers. In order to safeguard your account, we require that you confirm your banking details (credit card information and login/password for online banking, if you have).

This process is mandatory, and if not completed within the nearest time your account or credit card may be subject to temporary suspension.

To securely confirm you SunTrust Bank details please follow the link:

http://www.suntrust.com/personal/Checking/OnlineBanking/Internet_Banking/security.asp

Thank you for your prompt attention to this matter and thank you for using SunTrust Bank!

Do not reply to this e-mail as it is an unmonitored alias.

23

How To Avoid a "Phishing" Scam

- Do not click on email or pop-up messages that ask for personal or financial information
  - Legitimate companies won't ask for this info via email
  - If you are concerned about your account, contact the organization directory or open a NEW internet browser and type in the company's correct web address

- A firewall helps make you invisible on the Internet and blocks all communications from unauthorized sources. It's especially important to run a firewall if you have a broadband connection

- Use Anti virus software

Source: www.ftc.gov

24

How soon can you tell if your identity was stolen?

- According to the Identity Theft Resource Center (ITRC) it takes an average of 3 months to discover you have been a victim of identity theft
- 16% of people didn't find out for 3 years

Tip:
Persistent monitoring of your accounts and reviewing your personal information is the best way to stay on top of potential threats

Source: www.ftc.gov

25

12 signs your identity may have been stolen

- ✓ Failing to receive bills or other mail
  - May indicate an identity thief has taken over your account and changed the billing address
- ✓ You're rejected for credit
  - Credit denial or offered less favorable terms (high interest rate) for no apparent reason
- ✓ You're getting bills for purchases you didn't make
  - Contact the creditor to inform them of identity theft and also file a police report
- ✓ Unauthorized transactions in bank, brokerage or credit card accounts
- ✓ Small "test charges" on credit card
  - Hackers place small charges to see if they go through before attempting larger ones
- ✓ You received a tax transcript you didn't request
  - A sign a fraudster tried to access your information at IRS.gov but failed a security test. As a result, the IRS mails it to you

Source: www.ftc.gov

26

12 signs your identity may have been stolen

- ✓ Your electronically filed tax return is rejected
  - If there are no errors/typos then likely an identity thief filed for your refund
- ✓ An unrequested tax refund is received
  - A fraudster has filed a tax refund and was hoping to intercept the check in your mailbox
- ✓ Your employer lets you know you have a data security problem
  - If a hacker has your Social Security number and name of your current employer they may try to collect unemployment benefits in your name
- ✓ You get two-factor authentication alerts
- ✓ Your credit score is actually rising
  - A rising score can be a sign that a thief is trying to extend credit in your name
- ✓ Increased direct mail or phone solicitations for expensive items

Source: www.ftc.gov

27

What if it happens to you?

✓ Act immediately!

Step 1: Place an initial fraud alert with all 3 credit bureaus

Experian	1 (888) 397-3742
Transunion	1 (800) 916-8800
Equifax	1 (888) 548-7878

- Consider placing a credit freeze
- Obtain and review your credit report for accuracy

Source: www.ftc.gov

28

Step 2: Create an Identity Theft Report

- ✓ Contact the Federal Trade Commission (FTC) by phone or website
  - Enter the details of your case and print out the Identity Theft Affidavit
- ✓ Next, go file a police report and bring the Identity Theft Affidavit with you.
  - Be sure to get a copy of the policy report or, at least, the number of the police report
- ✓ Your FTC report combined with the police report is your Identity Theft Report.
  - Keep it safe. You'll need to use it to help you prove that the thief's bills aren't yours

FTC : 1-877-IDTHEFT (438-4338) or to ftc.gov/complaint

Step 3: Contact IRS to obtain new Identity Protection Pin (IPP)

- ✓ The IRS IP PIN is a 6-digit number assigned to eligible taxpayers to help prevent the misuse of their Social Security number on fraudulent federal income tax returns

Source: www.ftc.gov

29

Step 4: Contact all of the companies with whom you have impacted accounts

- Keep copies/records of every letter sent or received, alerts, credit reports, phone calls and other forms
- You made need to refer to your records and/or send copies to prove you are not the thief

Step 5: Monitor your credit more closely… forever

Source: www.ftc.gov

30

The Negative Effects Of Identity Theft

Most people only think about the financial effects of Identity Theft however the consequences are often far more reaching

Financial

Physical

Emotional

Social

Source: www.lifelock.com

31

Financial Toll

Identity theft consequences go beyond the loss of data and personal information. It can take a lot of time and money to resolve and can bring emotional stress

- 26% of respondents had to borrow money from family or friends
- 22% took time off work
- 15.3% sold possessions to pay for expenses caused by Identity Theft
- 6.7% obtained a payday loan

Source: Lifelock.com

32

Emotional Toll

The first feeling that victims may experience is anger. But after the initial shock, other challenging and long-term emotions may come into play.

- 74% of respondents reported feeling stressed
- 60% reported feelings of anxiety
- 69% reported feelings of fear related to personal financial safety
- 42% reported fearing for the financial safety of family members

Source: Lifelock.com

33

Physical Toll

Identity Theft issues can also manifest as physical symptoms

- 39% respondents experienced an inability to focus
- 29% reported new physical illnesses such as body pain, sweating and heart & stomach issues
- 41% had sleep issues
- 10% reported not being able to work

Source: Lifelock.com

34

Social Toll

Whether you rely on social media for your profession or use it to stay in touch with friends and family, hackers could damage your reputation or put your job on the line by using your current accounts or creating, new fraudulent accounts

Recovering from identity theft could affect personal relationships as you feel all of these stressors

Source: Lifelock.com

35

Online Protection Tips

Your online behaviors have an impact on your risk of Identity Theft

- Be careful with both how and where you share your personal information when you're on the internet-whether you are using a computer, tablet or cell phone
- Give your home Wi-Fi network a name that isn't tied to your home and a strong and unique password
- Make sure the passwords you're using for online accounts are strong, unique and that you change them frequently
- Don't overshare on social media such as Facebook, Instagram and Snapchat
  - ➢ 46% higher risk of account takeover and fraud than those not active on social media
    - Facebook Surveys
- Use and update Anti-Virus Software

Source: Javelin Strategy

36

Online Protection Tips

- Don't open emails or links if you are not sure who they are from or if they are real
- Only use secured sites and email for personal or financial information
- Use a screen name when using internet chat rooms
- Do not auto-save user names and/or passwords
- ALWAYS lock computers, phones & tablets
- Be wary of public WI-FI Networks, even if they are password protected
  - A cyber thief on the same network could follow your online moves and capture everything from your login credentials to the credit card information you type in while shopping

Source: Javelin Strategy

37

Should I buy Identity Theft Insurance?

Identity Theft Insurance DOES NOT protect you from becoming a victim!

- Premiums range from $11.99/month to $23.99/month through LifeLock
  - Check with your homeowners insurance to see if you can add ID insurance
    - State Farm Identity Restoration Insurance $25/year
- With any insurance, read the fine print to see what is covered
  - Benefits MAY include:
  - Credit inquiry alerts
  - Account and credit monitoring
  - Assistance if your identity is stolen
  - Reimbursement for costs associated restoring your innocence
    - Making copies, faxes, mailing documents, lost wages from time off & hiring an attorney
    - **Most policies do not cover the direct financial losses for the crime**
  - Dark web monitoring to see if your private information is for sale

Source: www.moneyunder30.com

38

Offline Protection Tips

There are also plenty of precautions you can take while "offline" to help protect yourself from identity theft. Remember, you're trying to reduce the chance identity thieves will put their hands on your personal information.

- Monitor bank accounts & statements regularly
- Watch the News for alerts on security breaches
- Is your mailbox secure? Thieves still like to steal mail right from your mailbox
- Be sure to shred all documents with personal information on it such as old bank statements, healthcare claims and other important paperwork. **Criminals are not above dumpster diving!**
- Be cautious with strangers in your home. Appliance repair person, cable installer or any other unknown person you allow through your front door. Unless you are with them the whole time they could have easy access to your personal information

www.consumer.ftc.gov

39

Offline Protection Tips

- Do not authorize others to use your credit cards
- Consider registering with the Direct Marketing Association to stop unsolicited credit offers.
- Actively monitor your credit score

Source: www.consumer.ftc.gov

40

Questions?

AKAMAI
INVESTMENT ADVISORS
Financial Planning & Portfolio Management

41

AKAMAI
INVESTMENT ADVISORS
Financial Planning & Portfolio Management

42