Elder Fraud Prevention & Cybersecurity in the Digital Age

Howard Tischler, CEO

Liz Loewy, COO

EverSafe

August 27, 2024

FinancialExpertsNetwork.com

Tips to Protect Against CyberFraud & Identity Theft

- What is cybersecurity and why is it important?
- Common cyberattacks - examples
- Offline activities which become cyberattacks
- Anatomy of a data breach - misconceptions
- What is social engineering?
- Assessing your digital health
- Best practices for safety and security
- Considerations for aging clients
- Considerations for caregivers
- Plan in advance in case there's a crisis
- What to do in case of:
  identity theft and/or financial exploitation

Why are we here?

What is Cybersecurity?

- ✓ Personal data, financial accounts, and benefits are only accessible to you & designated others
- ✓ Devices (computers, cellphones, tablets) are secure
- ✓ Networks are working properly and secure
- ✓ Network devices (ring doorbell, thermostat, TV) are secure
- ✓ Personal information is protected online & offline
- ✓ Vigilance is practiced as new risks appear (e.g. Zelle, Venmo, Paypal)

Common Cyberattacks

- Phishing – Trick people into giving up personal information
  - Email, Text, Popups
  - Tech Support Scams
- Open Wireless Networks – Home & Public Places (e.g. hotels)
- Viruses
  - Email Attachments, Popups
  - Video Streaming, Electronic Voicemail Messages
  - Appointments on your electronic calendar
- Swatting – Claim that you/your financial resources are involved in a crime
- Is it only about Cyber Threats?
  - Phone Phishing
  - Postal Mail (e.g. Phishing, Theft)

Elder Fraud: $36 Billion Problem

CHALLENGES FOR SENIORS & FINANCIAL PROFESSIONALS

Deep pockets + vulnerability:

- 83% of household wealth held by the 50+
- 1 in 3 seniors now dies with dementia

Financial institutions are not addressing this crisis:

- $120K average loss per victim
- $36K average loss to caregivers

6

Reasons for Under-reporting?

- Family members/Caregivers:
  largest percentage of exploiters
- Embarrassment & shame
- Guilt
- Loss of independence
- Diminished capacity

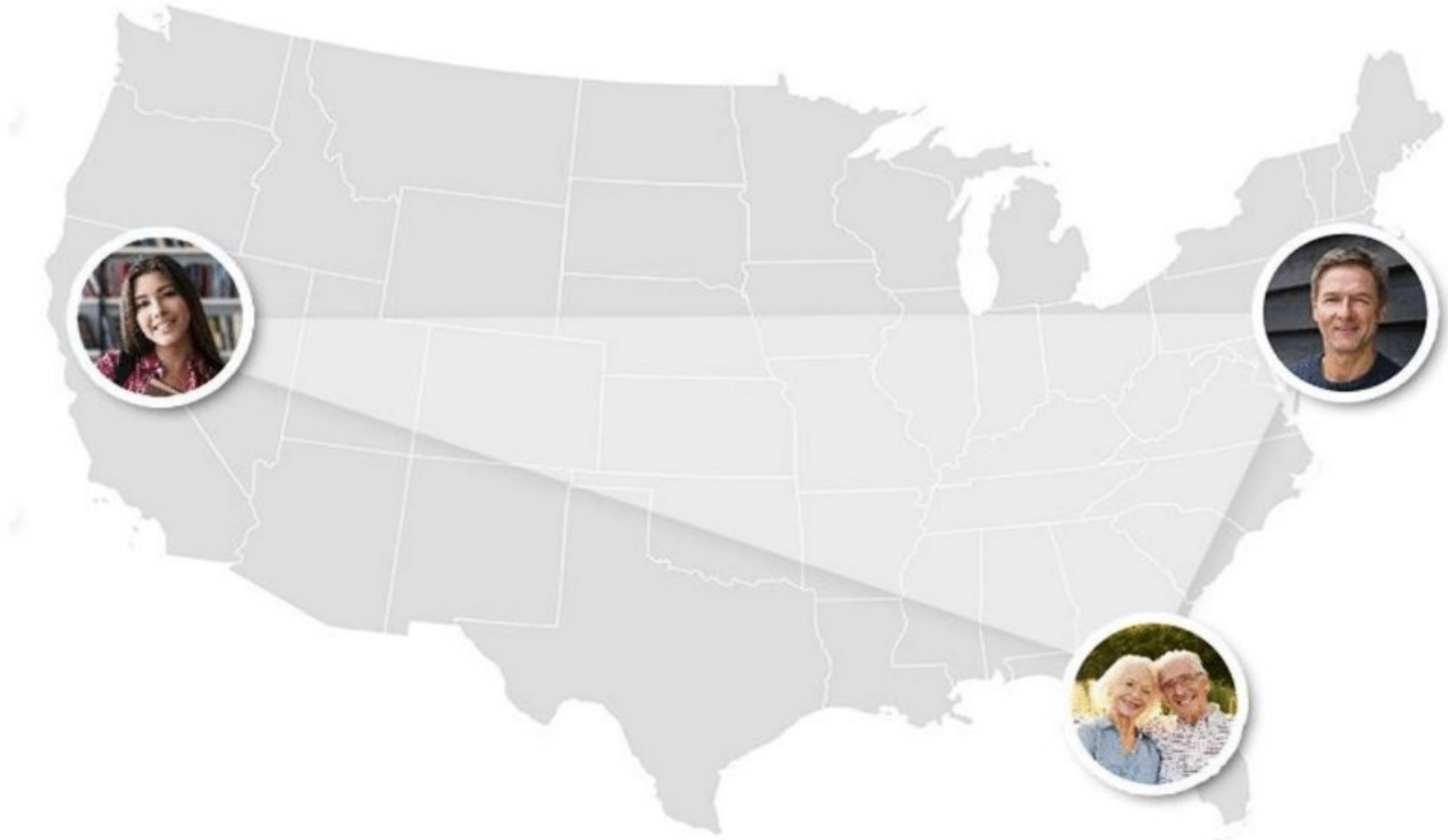
Challenges for Financial Institutions:
LIMITED SHARING OF INFORMATION

No Visibility Across Institutions

Static Alerts Unrelated to the Historical Behavior of Customer

Sharing of Information Restricted by Privacy Regulations

Challenges for Caregivers:
VISIBILITY & COMMUNICATION



Common Scams

Grandparent/ Imposter scams

Tax and debt collection scams

Charity scams

Telemarketer, mail offer or salesperson scams

Common Scams, cont'd

Paypal, bank, and Zelle scams

Crypto fraud and scams

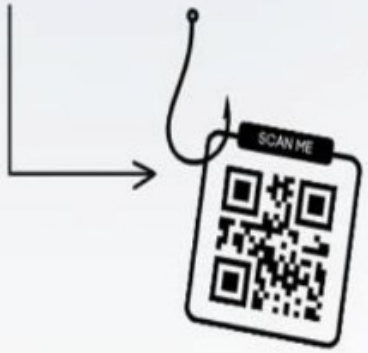
Romance scams

Lottery and sweepstakes scams

Newer Elder Scams Involve Cyber Threats

Digital Wallet Scams

- These scams are as common as they are straightforward.
- The fraudster simply texts or emails a phony invoice or payment confirmation that looks real, inducing the user to click a link, enter personal information, and/or respond to the scammer.



QR-Phishing

- Involves fraudsters generating fake QR codes that mimic legitimate ones.
- Fraudsters utilize QR codes to steal personal/financial information, either by pasting a phony QR code over a real one or sending their own QR code directly via text or email.
- Often tied to a free gift, new product, or necessary service.

Phantom Hackers

- A common scam that often ensnares unwitting users.
- The online user is warned that their computer has been attacked and their financial data has been exposed or used in a crime. Victims are directed to their purported "bank" and "law enforcement" and instructed to transfer funds that goes straight to the scammer.
- Funds are seldom recovered.

[redacted] Auth Support | 2FA Multifactor

[redacted] Re-authenticate 2 Factor Authentication (2FA) 19/Sep/2023 <info@morigen.org>

To [redacted]

Reply | Reply All | Forward

Tue 9/19/2023 11:56 AM

Microsoft

Dear User:

Your authenticator session has expired today. Kindly re-authentication with your mobile device to avoid being locked out of your email account.

Quickly Scan the QR Code below with your smartphone camera to re-authenticated your password security.

Regards,
Microsoft Support

This is an image, not text and not the real Microsoft logo.

It is how the scammer is bypassing Microsoft's detection.

Display the QR code on the phone – "r20.rs6.net"

Is Microsoft sending you to a website not related to Microsoft? NO

Forward unknown emails to hotline@EverSafe.com. Forward unknown texts/voicemails to 240.630.1990.

DO NOT CLICK ON ANYTHING IN UNKNOWN EMAILS/TEXTS OR CALL PHONE NUMBERS IN UNKNOWN EMAILS/TEXTS/VOICEMAILS.

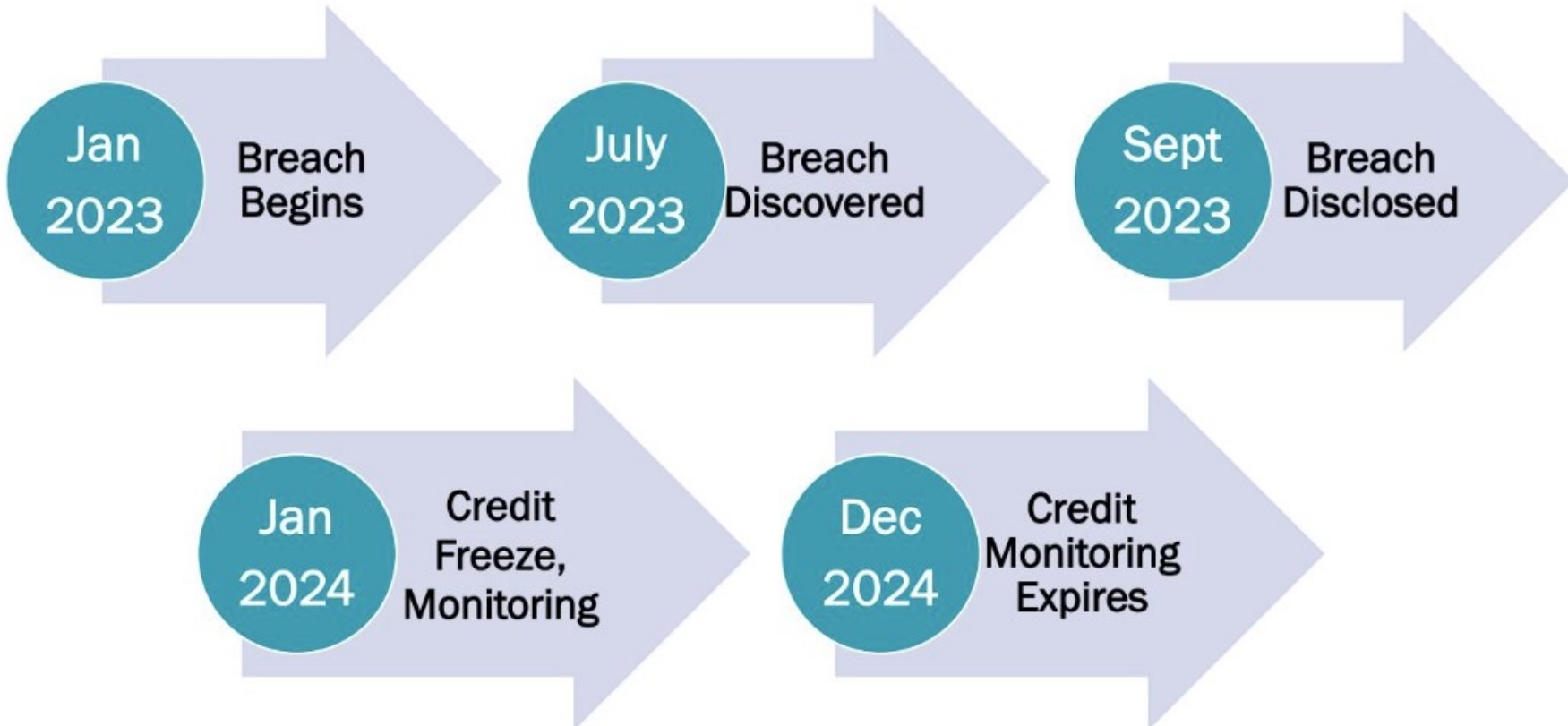
Who is at greater risk?

How phone spoofing works

1. Fraudster spoofs local phone number or information into caller ID device
2. Recipient is fooled into thinking the call is legitimate
3. Fraudster persuades the recipient to provide passwords or personal identifying information
4. Fraudster uses the information to:
   - Conduct account takeover
   - Perform social engineering
   - Implement account changes
   - Open new accounts
   - Make fraudulent purchases

Anatomy of a Data Breach

Have you ever been a victim of a breach?



Identity Theft: Latest Breaches

- MOVEit, AT&T, NPD, Change Healthcare/United Healthcare
- Most Americans affected
- MOVE it involved file transfers of sensitive data and “automated workflow automation”
- NPD left the password to their database exposed – after the breach

Dark Web? Open Web?

What is the Dark Web?

Part of the Web only accessible by special software, allowing users/websites to remain anonymous or untraceable

Why is it important?

Dark Web is the online marketplace for hacked data

What is the Open Web?

Part of the Web accessible by general public via web browser
(e.g. Google, Bing, Yahoo, etc)

Why is it important?

Online marketplace for publicly available data +
Data purchased on the Dark Web = Comprehensive profile on an individual

What is Social Engineering

- Cybercriminals use information commonly available through …
  - Social Media
  - Location Sharing
  - In-person Conversations
  - Legitimate Marketing Data Bases
  - Dark Web
- Every piece of information is a stepping stone to more information
  - Combined from a variety of sources
  - Can start from a phone call, facebook, bio on company website, trash, …

Open Web – Available Data

- Name
- Birth Date
- Gender
- Ethnicity
- Education
- Occupation
- Marital Status
- Political Party
- Residential Details
- Home Value
- Mortgage Info
- Home Equity Info
- Vehicle Info
- Relatives
- Mother's Maiden Name
- Father's Middle Name
- Children's Name(s)
- Children's Birth Date(s)
- Income
- Credit Card Types
- Purchase Frequency
- Open Credit
- Types of Purchases
- Purchase Categories ($)
- Internet Provider
- Cable Provider
- Phone Number(s)
- Address(es) & History
- Employer & History
- Aliases
- Neighbors
- Email Address(es)
- Social Networks
- Marriage(s) & Divorce(s)
- Liens/Bankruptcies
- Lawsuits
- Interests
- Personal Computer Type
- Types of Vacations

Assessing Your Digital Health

Digital hygiene - **best practices to help keep your digital life "healthy"**

1. Do you keep your software up-to-date?
2. Is your anti-virus up-to-date & scan turned on?
3. Is your home router secure?
4. Do you use strong passwords and only use them once?
5. Do you use two-factor authentication?
6. Do you only download software from legitimate sites?
7. Do you open emails/texts from unknown sources?
8. Do you limit information sharing on your social media accounts?
9. Do you shred documents containing personal information?
10. Do you use unprotected network connections in hotels?

Ways to Protect Yourself

- ✓Avoid common words (e.g. names, locations, hobbies), complex
- ✓Unique passwords for EVERY important account
- ✓Two-factor authentication (e.g. online access to cell phone, apps)
- ✓Password manager

Ways to Protect Yourself - 2

- Software updates are essential (computers & phones): new vulnerabilities are found every day (450,000 released daily)
- Anti-virus software
- Protect your home
- Use a Virtual Private Network (VPN) when on the road
- Establish online access to all accounts & benefits (fight fire w/fire)
- If you connect it, protect it: update doorbells, thermostats, Alexa, health monitors

Ways to Protect Yourself - 3

- Scrutinize unexpected emails (i.e. bank, Paypal/Zelle/Venmo, Amazon)
- Don't click it
  - Unsure of an email (forward it to hotline@EverSafe.com)
  - Unsure of a text/voicemail (forward it to 240.630.1990)
- Avoid unexpected attachments
- Avoid phone numbers in unexpected emails
- Utilize a robocall blocker (e.g. Nomorobo, YouMail)
- Beware of free apps on your phone
- Shred documents

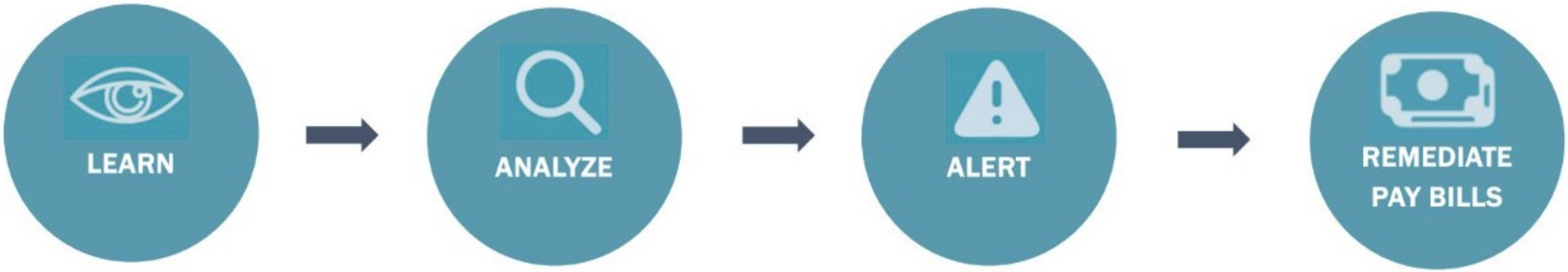
Use Technology: Fight Fire With Fire!

PROMISING INTERVENTIONS

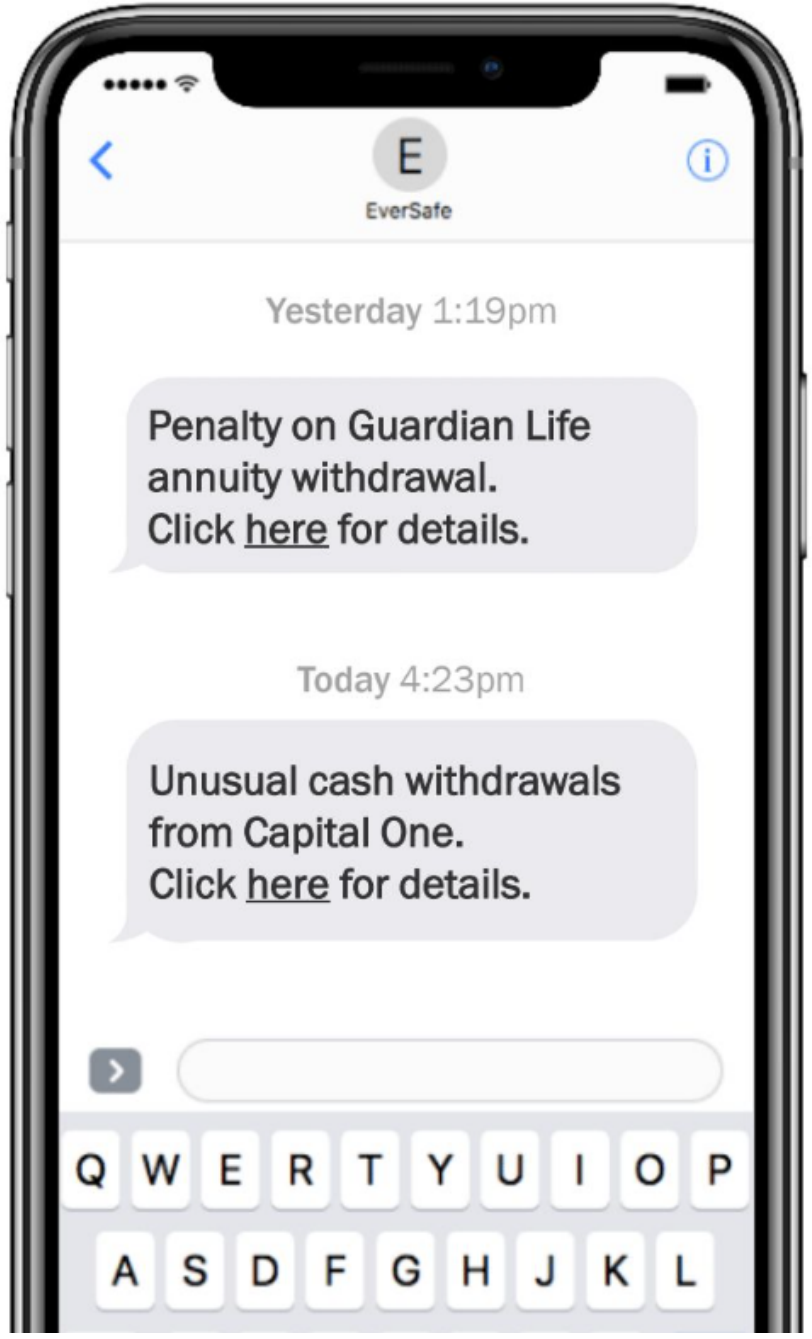
- SAR – Flag box
- Monitor across accounts, institutions w/alerts to trusted contacts
- Tech-enabled bill pay
- Call-monitoring
- Pre-paid debit card
- Digital safe
- Reporting initiative: HelpVul

EVERSAFE

AN 'EXTRA SET OF EYES'

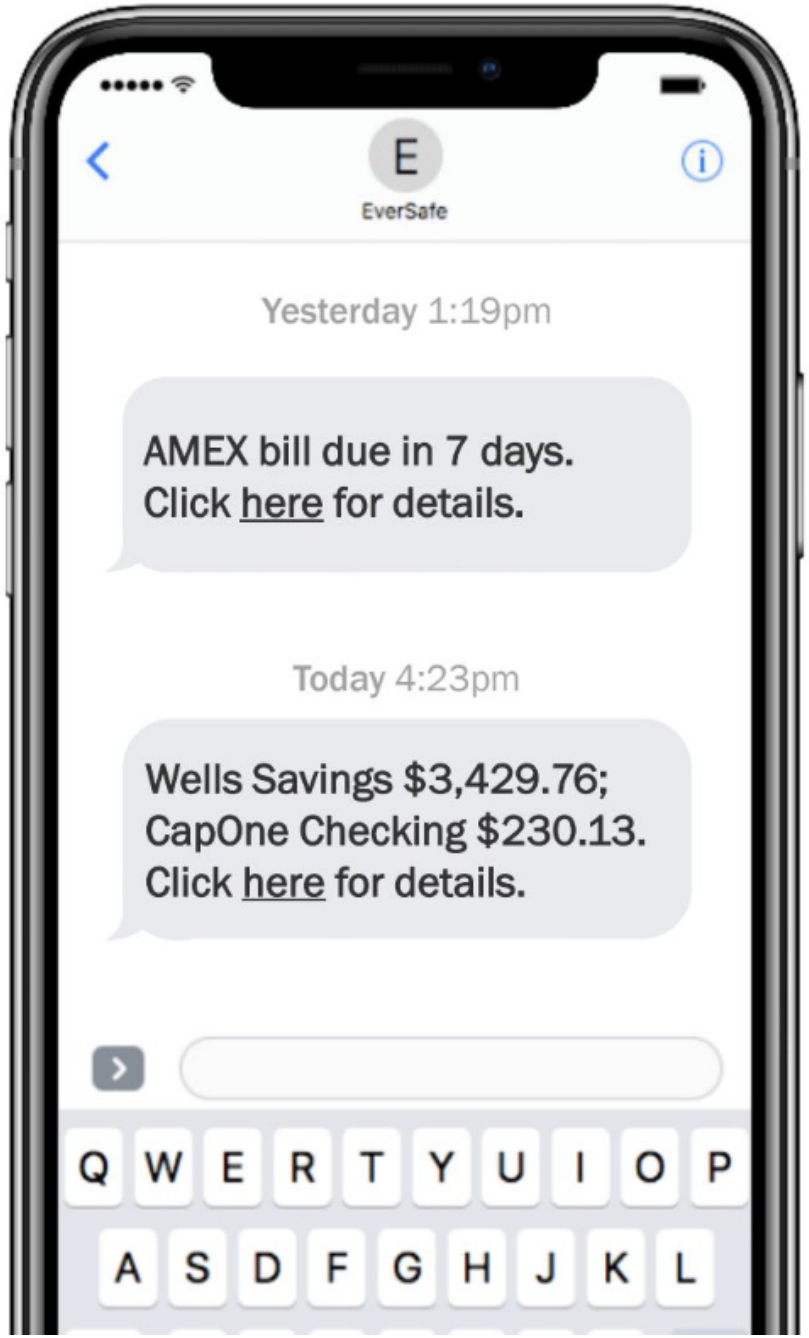


- Analyzes Financial Accounts Across Institutions, Credit & Real Estate
- Identifies Behavioral Changes & Anomalies (Machine Learning)
- Alerts Members, Caregivers, Loved Ones & Professionals
- Tracks Issues to Resolution & Provides Remediation Support



Personalized Alerts

- Change in spending
- Missing deposit
- Unusual wire transfer
- Abnormal ATM/ACH activity
- Real estate title changes
- Dormant account activity
- Over/under-payment on bill
- Erratic investment activity
- Address change on account
- New/changed property liens



Stay on Top of Family Finances

- Account Balances
- Upcoming/Late Bills
- Payment Processing
- Home Valuation
- Interest Rate Changes
- Credit Limit Adjustments
- Recurring Charges
- Subscription Renewals

HELPVUL

- **Goals:**
  - Uniform, efficient & secure reporting
  - Protected document-sharing
  - Improved identification & investigation of referrals involving suspected exploitation of at-risk adults
  - Enhanced communication & efficiency
- **Partners**
  - National Adult Protective Services Association (NAPSA)
  - Securities Industry & Financial Markets Association (SIFMA)
  - EverSafe
- **Live:**
  - North Carolina, Missouri, Montana, Pennsylvania, California, Florida. Georgia, more on the way…
  - 67 financial institutions
  - Target: All States, Banks, Broker-Dealers, Credit Unions

Considerations for Aging Clients

- As tech devices have grown in use with aging clients, there has been a surge in cybertheft & scams
- 61% own smart phones & 75% surf the net[1]
  - Only 26% feel “very confident” using computers & smartphones
- Even when aware of the danger, most don’t believe they will be a victim & underestimate the havoc it can cause
  - 90% believe seniors are targeted, 10% believe it will happen to them[2]
- Stick to who you know; loved ones can help – especially if traveling

[1] Pew Research
[2] Wells Fargo study

I'm a Caregiver – How Can I Help?

- Have a conversation about common scams, unexpected emails/texts
- Establish strong passwords, online banking access (even if not used)
- Ensure private settings on social media, if used
- Freeze the loved ones' credit (most no longer need credit)
- Sign up for digital monitoring of postal mail
- Install robo-blocking utilities on land lines & cell phones
  Educate: don't answer unknown phone numbers; if do, hang up immediately
- Have loved one enroll in for EverSafe – w/you as a 'Trusted Advocate'

Cybersecurity Awareness

People are too “smart” to be victims

- Seniors: 90% believe they’re targets, 10% believe they’ll be victimized (Wells Fargo)

Once victimized - too “smart” to “fall” for it again

- Previous victims are prime targets & will be victims again

We worry about you, but are even more worried about those not here

- Think about yourself, your loved ones, your friends

What to do In Case of a Breach:

- Review all credit & consumer reports
  Equifax, Experian, Trans Union, Early Warning, Chexsystems, NCTUE
- Freeze your credit, Chexsystems, NCTUE
  You can always unfreeze your credit when you need it
- Ensure you have online access established for financial institutions, social security, other benefits, cell phone account(s), IRS
- Request a PIN from the IRS, if you don't already have one
- Be vigilant about familiar & unfamiliar texts/emails/phone calls
- Sign up for EverSafe

Creating a Safety Net

Fraud Alert

EQUIFAX
800-525-6285

EXPERIAN
888-397-3742

TRANSUNION
800-680-7289

FREE CREDIT REPORT
annualcreditreport.com

Credit Freeze

EQUIFAX
www.equifax.com/personal/credit-report-services/

EXPERIAN
www.experian.com/freeze

TRANSUNION
www.transunion.com/credit-freeze

Opt Out of Marketing Solicitations

DO NOT CALL LIST
donotcall.gov/
1-888-382-1222

CREDIT BUREAUS
optoutprescreen.com

ACXIOM
isapps.acxiom.com/optout/optout.aspx

DIRECT MARKETING ASSOCIATION
dmachoice.org

COMMERCIAL MARKETING MAIL
www.lexisnexis.com/privacy/directmarketingopt-out.aspx

BLOCK ROBO CALLS
nomorobo.com
youmail.com

COMMERCIAL MARKETING EMAIL
www.ims-dm.com/cgi/optoutemps.php.

Financial Protection

IDENTITY THEFT & FINANCIAL MONITORING	www.EverSafe.com (Contact your advisor for your promotion code)
PRE-PAID DEBIT CARD	www.truelinkfinancial.com
LEGACY DIGITAL ASSETS	www.digitalcommunications.com
MANDATORY REPORTING CHART	www.EverSafe.com/Mandatory-Reporting

EVERSAFE

Distribution Options

Advisor Pay (Unlimited Clients)

- Gold Plan $199/month/advisor
- Includes Spouse/Partner
  (Additional family members - 25% discount)
- Advisors, Complimentary
- Options
  - Real Estate $3.99/month/property
  - 401K Institutional Clients

Client Pay

- 20% Discount
- 30 Day Free Trial
  (Additional family members - 25% discount)
- Advisors, 1 Year Complimentary
- Options
  - Real Estate $4.49/month/property

Advisor Registration

- Visit www.EverSafe.com/Advisors
- Enter registration code Special24
- Select Advisor Pay (“Unlimited Program”) or Client Pay
- Enroll yourself
- Client enrollment
  - Advisor pay: you will receive a unique link for your clients
    - *Enables you to view enrolled clients*
  - Client pay: you will receive a unique link for your clients

Call 888.575.3837 or email advisors@EverSafe.com

www.EverSafe.com

4701 Sangamore Road #100N
Bethesda, MD 20816

21 West 46th St, 16th Floor
New York, NY 10036

Howard Tischler
htischler@eversafe.com
(888) 575-3837 x-701

Liz Loewy
eloewy@eversafe.com
(888) 575-3837 x-702