



## Internal Processes and Digital Solutions to Combat Wire Fraud



### **Charles (Chas) W. Smith, III**

Assistant Vice President | Mississippi Valley Title Services Company

Assistant Vice President | Old Republic National Title Insurance Company

Agent Representative | Business Development | Associate Counsel



**The information provided is for informational purposes only and should not be used or relied upon for any other purpose. This information is not intended nor should it be construed as providing legal advice. Old Republic National Title Insurance Company does not guarantee, and assumes no responsibility for, the accuracy, timeliness, correctness, or completeness of the information. Always seek the advice of competent counsel with any questions you may have regarding any legal issue.**



# Outline

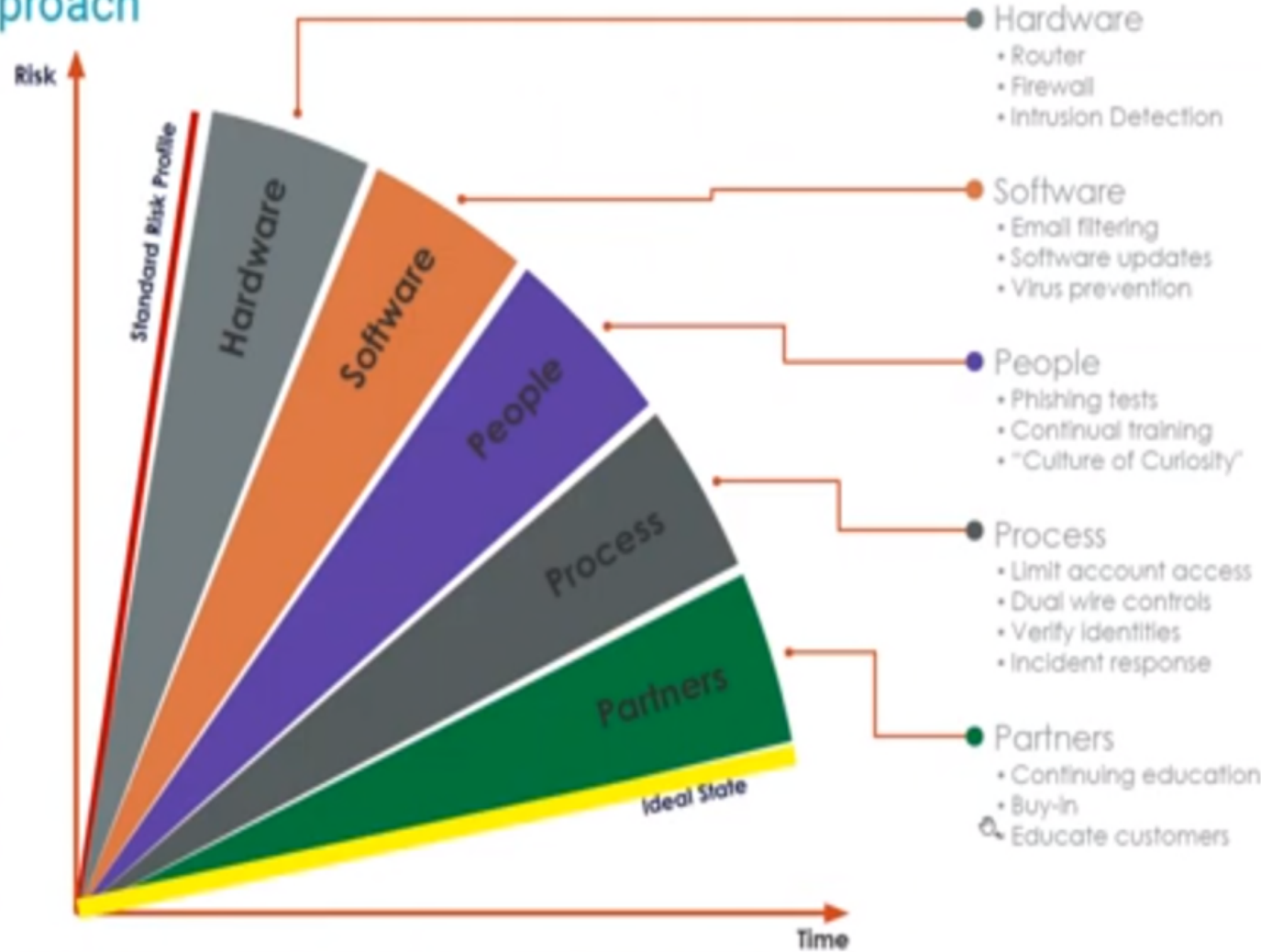
- I. Why is Wire Fraud So Prevalent?
- II. Know Your Network
- III. Alabama Trust Account Law, Ethical Rules, Alabama Data Breach Law and Recent Data Breaches
- IV. Understanding the Weakest Link
- V. Training For Prevention
- VI. Working With Like-Minded

# I. Why is wire fraud so prevalent

- It's LUCRATIVE
- FBI reports show US losses of around \$3 Billion Dollars per year in wire fraud
- Wire fraud losses globally are around \$12.5 Billion Dollars per year
- In 2018 there were 11,300 cybercrimes reported to the FBI's Internet Crimes Control Center totaling nearly \$150 million in losses involving real estate fraud
- Average Bank robbery is around \$7,000 and the average wire fraud loss is around \$137,000
- ALTA reports that 75% of title agents do not conduct phishing test

# Ideal Target to Ideal State

## A Layered Security Approach



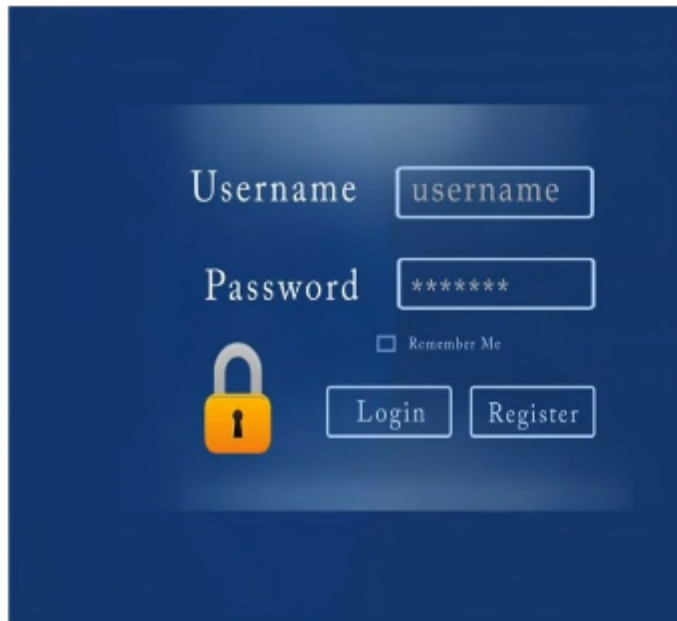
## II. Know Your Network

- Understand and protect against the “threat landscape”
- Your perimeter consists of:
  - Passwords
  - Email
  - Wi-Fi
  - Hardware (cloud)
  - Software/Apps

# Passwords: Your First Line of Defense

- Use phrase passwords with numbers and special characters (ex. Oh my, 1 stubbed my toe!)
- Password length should be at least 16 characters long
- Use a password manager like Lastpass, Dashlane or 1Password
- NEVER give out your password to anyone


# Password Security



Username

Password

Remember Me



Length of Password

Password Reuse

Keystroke Logging

Brute Force Attack

Data Breach



# Is your Password on this List?

SplashData, maker of password manager applications, released this list of the 25 most used password in 2018.

123456	welcome
password	666666
123456789	abc123
12345678	football
12345	123123
111111	monkey
1234567	654321
sunshine	!@#\$%^&*
qwerty	charlie
iloveyou	aa123456
princess	donald
admin	password1
	qwerty123

# 2FA: An Added Layer of Protection

- Two Factor Authentication (2FA) can be added to your email account and other personal accounts like LinkedIn
- It will require you to enter a code sent to your phone or e-mail.
- Beware: 2FA portals can be spoofed like an email or website
- 2FA is still considered a best security practice

# Email

- Emails are not secure
- Communication protocol used by email called Simple Mail Transfer Protocol (SMTP) doesn't involve authentication.
- Attachments can be dangerous (ransomware, malware, etc.)
- Learn and teach signs of email spoofing

# Common Cybersecurity Schemes



**Email Account Compromise**



**Ransomware**

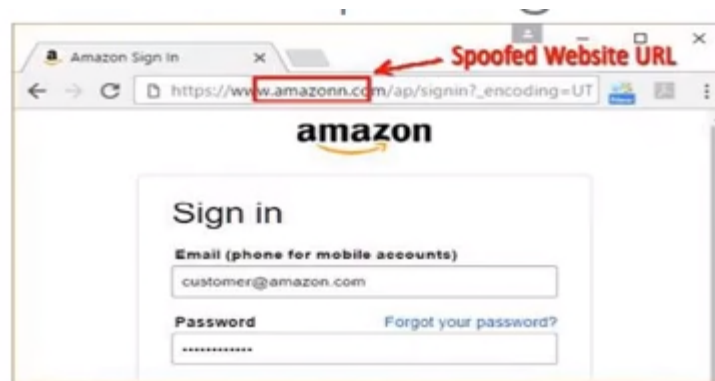


**Viruses, Spyware & Malware**



# Playing Detective

- Website portal spoofing
- Unsecure websites are fabricated websites made to deceive the user into inputting their information.



Review Expenses - Message (HTML)

FILE MESSAGE GpgOL

Ignore Delete Reply Reply All Forward Meeting IM More

the fan To Manager Team Email Rules Actions Move

Mon 27/04/2015 10:00

Finance <finance@finance-sophos.net>

Review Expenses

To

You forwarded this message on 27/04/2015 10:01.

Message expenses\_submission.xlsx (38 KB)

Hi,

Please can you review your recent expense claim that I've attached?

Let me know if you are happy with it or if you have any issues that need to be addressed.

Thanks,  
Finance

The image shows a Microsoft Excel window with a 'Security Alert' dialog box open. The dialog box contains the following text:

**Security Alert**

The identity of this web site or the integrity of this connection cannot be verified.

- ✓ The security certificate is from a trusted certifying authority.
- ✓ The security certificate date is valid.
- ⚠ The name on the security certificate is invalid or does not match the name of the site

Do you want to proceed?

Buttons: **Yes**, No, View Certificate

The 'Enable Content' button in the ribbon is also circled in blue. Below the dialog box, a red banner reads: "To view your expenses online, please click 'Enable Content' above."

A 'Network Credentials' dialog box is also open, asking for a username and password to retrieve a claim. The 'Submit' button is circled in blue.

## Email Account Compromise Can you spot a fake email?

After all, it doesn't say  
"I'm a fake"





# Top 5 Email Security Tips

1. Don't trust the display name
2. Look but don't click
3. Analyze the salutation
4. Don't give up personal information
5. Beware of urgent or threatening language

# Ransomware



- Malware is installed on the victim's computer that encrypts all the drives and files on the computer.
- The criminal requires the victim pay a ransom to obtain the decryption key.
- Key Focus
  - Prevention
  - Business continuity
  - Remediation

# Scams and Tactics



## Example 1

- Perpetrators obtain personal information on buyers
- Sets up fraudulent email addresses, phone and fax numbers
- Calls the buyer before the title company does
- Instills pressure to wire closing costs immediately, often includes threat they won't close on time
- Follows up with email that contains bogus wire instructions
- Buyer wires money and it goes to an offshore account

## Example 2

- Scammers obtain personal information on real estate agents
- Sets up fraudulent email addresses
- Sends fraudulent referral business emails to other real estate agents
- Real estate agent clicks on the link provided in the email and a virus designed to steal personal information is installed on their computer

# Wi-Fi

- Open Doors of Wi-Fi
  - Be sure to be connected to the correct Hotspot
  - Criminals can spy on your connection as well as hijack your files directly despite other securities
  - Use security on your internal WiFi, preferably WPA2
  - Update Routers with patches and upgrade the device very few years
  - Encryption of files and emails is important for this reason

# Encryption

- Process of encoding messages or information in such a way that only parties with the decryption key can read the data
- Full Disk Encryption is NOT enough
- Full disk encryption protects data that resides on your computer in case it is lost or stolen
- It doesn't protect the information when it is in transit, stored on the cloud or infected with data stealing malware
- File Encryption is a tool that encrypts a file as soon as the file is created. Various software tools offer this

# Hardware

- Hardware-based security includes
- Desktop and laptop computers, USB drives, routers
- Use a leading Next Generation Firewall with the following capabilities – Intrusion Prevention (IPS) using deep packet inspection, Advanced Threat Protection (ATP), Sandboxing, GeoIP filtering, Web / Application protection with https scanning, works in conjunction with Endpoint Protection agent.

# Software/Apps

- Know your source when downloading software/apps
  - Get apps via your mobile device's official marketplace
  - Check the mobile app reputation (rating) of the developer
- Update software with latest patches
  - Ensure your installed apps and software are up-to-date
  - Microsoft is no longer providing patches for Explorer
    - Switch to using Microsoft Edge
- Use advanced Endpoint Protection software
  - Specific ransomware protection, exploit prevention, ML
  - Works in conjunction with the firewall

# Our “Digital Distance” Exposes Everyone Watch





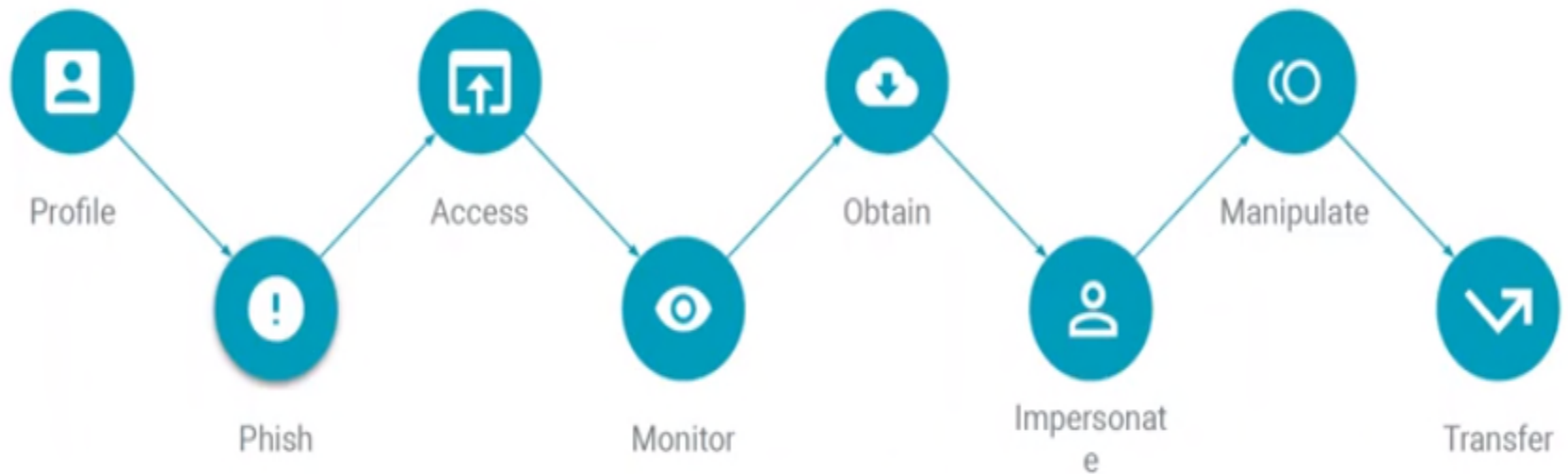
# Possibilities

Every day, an estimated 30,000 Americans & 80,000 Canadians fall for an email phishing scam.

~7,500 successful fake invoice phishing attacks per day in the USA.



# Steps to Committing Fraud



# Estate Fraud

- Monitor death certificates filed in affluent counties across the county
- Identify a recently deceased individual who owned property at the time of death
- Impersonate a PR of the deceased and then fake court documentation authorizing the sale
- List and steal property or divert earnest money in connection with a buy/sell arrangement.

# Who is Responsible for Wire Fraud Losses

- Plaintiff was granted judgment against Defendants (Broker and Agent) jointly and severally, on his claim for negligent misrepresentation in the amount of \$167,129.27
  - Bain v. Platinum Realty LLC et al. Case No. 16-DV-02326  
JWL Dist. Court, D. Kansas 2019

# Trust Accounts

## Rule 1.15

- A lawyer shall hold the property of clients or third persons that is in the lawyer's possession in connection with a representation separate from the lawyer's own property. Rule 1.15(a), Alabama Rules of Professional Conduct.
- A lawyer shall designate all trust accounts, as well as checks and deposit slips, as an "Attorney Trust Account".
- Complete records of such account funds and other property shall be kept by the lawyer and shall be preserved for six (6) years after termination of the representation. Rule 1.15(e), Alabama Rules of Professional Conduct.

## Recent Data Breaches

- **Marriott International (November 30, 2018)**

Marriott International disclosed a security breach of the reservations system for its Starwood Hotels and Resorts brand. The hack may have compromised private information on up to 500 million guests.

According to Marriott, the database included such personal information as name, mailing address, phone number, email address, passport number, date of birth, and gender for around 327 million Starwood guests. For some Starwood customers, the hacked database also stored payment card numbers and expiration dates, although Marriott has said that information was encrypted.



Source: [https://www.privacyrights.org/data-breaches?title=&org\\_type%5B%5D=261](https://www.privacyrights.org/data-breaches?title=&org_type%5B%5D=261).

## Recent Data Breaches (cont'd)

- **Panera Bread (April 2018)**

KrebsOnSecurity discovered that Panera Bread left millions of customer sign-up records (possibly 37 million) in plain text on its website, including email addresses, home addresses, phone numbers, and loyalty account numbers.

There was no payment information in the plain text, but it would have been easy for cybercriminals to harvest that information and use it as part of identity fraud or spam campaigns.



Source: [https://www.privacyrights.org/data-breaches?title=&org\\_type%5B%5D=261](https://www.privacyrights.org/data-breaches?title=&org_type%5B%5D=261).

## Law Firm Data Breaches - What is the Risk?

- 22% of law firms experienced a cyberattack or data breach in 2017 – up from 14% in 2016.
- 11% of law firms had to notify their clients of a data breach in 2017 and 17% reported an incident to law enforcement.
- Firms with 10-49 attorneys were most frequently attacked (35%), followed by firms of 50-99 attorneys (33%) and firms of 2-9 attorneys (27%). 23% of large firms with 500 or more lawyers were attacked. Solos had the lowest incidence at 10%.

Source: ABA 2017 Legal Technology Survey.



# Alabama Data Breach Law

Alabama Data Breach Notification Act of 2018, Ala. Code §§ 8-38-1 *et seq.* (effective June 1, 2018).



---

## AL Data Breach Law - Coverage

**Covered Entities - What entities are covered under or subject to the AL Data Breach Law?**

***Covered entities that acquire or use sensitive personally identifying information.***

---

A "covered entity" includes any person, sole proprietorship, partnership, government entity, corporation, nonprofit, trust, estate, cooperative association, or other business entity that acquires or uses sensitive personally identifying information. Ala. Code § 8-38-2.

# AL Data Breach Law – Notification Requirements

## When is notice to state residents required?

- A covered entity *that is not a third-party agent* that determines that as a result of a breach of security, sensitive personally identifying information has been acquired or is reasonably believed to have been acquired by an unauthorized person, *and is reasonably likely to cause substantial harm to the individuals to whom the information relates*, must give notice of the breach to each individual. Ala. Code § 8-38-5.
- An "individual" includes any Alabama resident whose sensitive personally identifying information was, or the covered entity reasonably believes to have been, accessed as a result of the breach. Ala. Code § 8-38-2.



# AL Data Breach Law - Breach

**Definition of "Breach"/Notification Trigger - What is/is not considered a breach of security triggering the requirement to provide notice to affected residents of the state?**

***Breach = unauthorized acquisition of data in electronic form containing sensitive personally identifying information.***

---

"Breach of security" or "breach" refers to the unauthorized acquisition of data in electronic form containing sensitive personally identifying information. Acquisition occurring over a period of time committed by the same entity constitutes one breach.

The term does not include any of the following:

- (1) Good faith acquisition of sensitive personally identifying information by an employee or agent of a covered entity, unless the information is used for a purpose unrelated to the business or subject to further unauthorized use.
- (2) The release of a public record not otherwise subject to confidentiality or nondisclosure requirements.
- (3) Any lawful investigative, protective, or intelligence activity of a law enforcement or intelligence agency of the state, or a political subdivision of the state.

"Data in electronic form" includes any data stored electronically or digitally on any computer system or other database, including, but not limited to, recordable tapes and other mass storage devices.

Ala. Code § 8-38-2.

# AL Data Breach Law – What is Sensitive PII?

## Definition of Personal/Protected Information - What types of information are protected under the AL Data Breach Law?

### *Sensitive personally identifying information.*

---

An AL resident's first name or first initial and last name in combination with one or more of the following with respect to the same AL resident is considered to be "sensitive personally identifying information":

- (1) A non-truncated Social Security number or tax identification number.
- (2) A non-truncated driver's license number, state-issued identification card number, passport number, military identification number, or other unique identification number issued on a government document used to verify the identity of a specific individual.
- (3) A financial account number, including a bank account number, credit card number, or debit card number, in combination with any security code, access code, password, expiration date, or PIN, that is necessary to access the financial account or to conduct a transaction that will credit or debit the financial account.
- (4) Any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional.
- (5) An individual's health insurance policy number or subscriber identification number and any unique identifier used by a health insurer to identify the individual.
- (6) A user name or email address, in combination with a password or security question and answer that would permit access to an online account affiliated with the covered entity that is reasonably likely to contain or is used to obtain sensitive personally identifying information.

## AL Data Breach Law – What is Not Sensitive PII?

The term “sensitive personally identifying information” does not include either of the following:

- (1) Information about an individual which has been lawfully made public by a federal, state, or local government record or a widely distributed media.
- (2) Information that is truncated, encrypted, secured, or modified by any other method or technology that removes elements that personally identify an individual or that otherwise renders the information unusable, including encryption of the data, document, or device containing the sensitive personally identifying information, unless the covered entity knows or has reason to know that the encryption key or security credential that could render the personally identifying information readable or useable has been breached together with the information.

# AL Data Breach Law – Notification

**When must notice be provided to residents of the state?**

***Notice must be provided as expeditiously as possible and without unreasonable delay, but must be provided within 45 days of notice or determination of breach.***

- 
- Notice to individuals must be made as expeditiously as possible and without unreasonable delay, taking into account the time necessary to allow the covered entity to conduct an investigation.
  - Unless a law enforcement delay is in place, a covered entity must provide notice *within 45 days of the entity's receipt of notice from a third party agent that a breach has occurred or upon the entity's determination that a breach has occurred and is reasonably likely to cause substantial harm to the individuals to whom the information relates.*



# AL Data Breach Law – Notice Content Requirements

The notice must include, at a minimum, all of the following:

- (1) The date, estimated date, or estimated date range of the breach.
- (2) A description of the sensitive personally identifying information that was acquired by an unauthorized person as part of the breach.
- (3) A general description of the actions taken by a covered entity to restore the security and confidentiality of the personal information involved in the breach.
- (4) A general description of steps an affected individual can take to protect himself/herself from identity theft.
- (5) Information that the individual can use to contact the covered entity to inquire about the breach.



# AL - Other Notification Requirements?

**Other Notification Obligations - Does the AL Data Breach Law require that notification of the breach be sent to the Attorney General, law enforcement, credit reporting agencies, regulators, or others?**

***Yes; notification to Attorney General and credit reporting agencies may be required.***

---

## **Attorney General Notification Requirements:**

If the number of individuals a covered entity is required to notify exceeds 1,000, the entity must provide written notice of the breach to the Attorney General as expeditiously as possible and without unreasonable delay.

# AL AG Notification Requirements

Written notice to the Attorney General must include all of the following:

- (1) A synopsis of the events surrounding the breach at the time that notice is provided.
- (2) The approximate number of individuals in the state who were affected by the breach.
- (3) Any services related to the breach being offered or scheduled to be offered, without charge, by the covered entity to individuals, and instructions on how to use the services.
- (4) The name, address, telephone number, and email address of the employee or agent of the covered entity from whom additional information may be obtained about the breach.

A covered entity may provide the Attorney General with supplemental or updated information regarding a breach at any time.

Information marked as confidential that is obtained by the Attorney General in connection with this notification process is not subject to any open records, freedom of information, or other public record disclosure law. Ala. Code § 8-38-6.

Note: A template Attorney General notification form was not included in the AL Data Breach Law.

# AL - CRA Notification Requirements

## **Consumer Reporting Agency Notification Requirements:**

If a covered entity discovers circumstances requiring notice to more than 1,000 individuals at a single time, the entity must also notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined in the Fair Credit Reporting Act, 15 U.S.C. § 1681a, of the timing, distribution, and content of the notices. Ala. Code § 8-38-7.

# AL – Credit Monitoring Services

**Does the AL Data Breach Law require covered entities to provide credit monitoring services to affected residents?**

***No, but if credit monitoring services are offered to impacted residents without charge, the required written notice to the Attorney General must describe these services.***

---

If the number of individuals a covered entity is required to notify exceeds 1,000, the entity must provide written notice of the breach to the Attorney General as expeditiously as possible and without unreasonable delay.

Written notice to the Attorney General must include all of the following:

- (1) A synopsis of the events surrounding the breach at the time that notice is provided.
- (2) The approximate number of individuals in the state who were affected by the breach.
- (3) ***Any services related to the breach being offered or scheduled to be offered, without charge, by the covered entity to individuals, and instructions on how to use the services.***
- (4) The name, address, telephone number, and email address of the employee or agent of the covered entity from whom additional information may be obtained about the breach.

Ala. Code § 8-38-6.

# American Bar Association Guidance

- On October 17, 2018, the American Bar Association Standing Committee on Ethics and Professional Responsibility released Formal Opinion 483 that reaffirms the duty of attorneys to notify clients of a data breach and details the reasonable steps attorneys may take to meet the obligations set forth by ABA model rules.
  - *“Not every cyber episode experienced by a lawyer is a data breach that triggers the obligations described in this opinion. A data breach for the purposes of this opinion means a data event where material client confidential information is misappropriated, destroyed or otherwise compromised, or where a lawyer’s ability to perform the legal services for which the lawyer is hired is significantly impaired by the episode.”*
-

# III & IV. Humans are the weakest link

- Creating a Culture of Compliance and Curiosity
- Security is everyone's job
- Use fraud attempts as training opportunities
- Train and empower employees and referral partners
- Test, measure, improve
- Celebrate wins
- Download a training guide: <https://certifid.com/ebook-clear-to-close/>

# Action Item: People

- Phishing Tests

- Free test by Google: <https://phishingquiz.withgoogle.com/>
- FTC Phish Quiz:  
<https://www.ftc.gov/tips-advice/business-center/small-businesses/cybersecurity/quiz/phishing>
- Third party phishing experts

- Password Managers

- LastPass (<https://www.lastpass.com/hp>)
- 1Password (<https://1password.com/>)

# Action Item: Process

- FTC - "Start with Security" Guide:  
<https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business>
- Response Plan
  - ALTA Rapid Response Plan:  
<https://www.alta.org/file.cfm?name=ALTA-Rapid-Response-Plan-for-Wire-Fraud-Incidents>
  - When Minutes Matter - Fraud Recovery Whitepaper:  
<https://certifid.com/when-minutes-matter/>
- Password Managers
  - LastPass (<https://www.lastpass.com/hp>)
  - 1Password (<https://1password.com/>)

 American Land



# Victim Response to Email Account Compromise Scheme

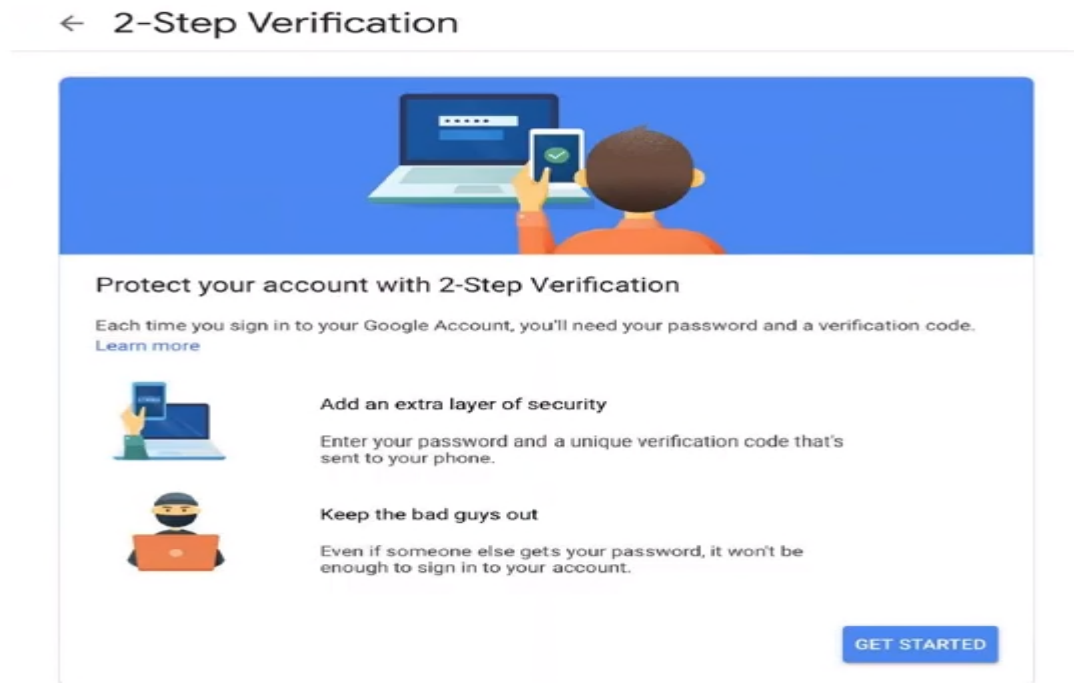
- 1 Notify your bank and the corresponding bank
- 2 Notify local FBI office and file a complaint with IC3
- 3 Consider civil injunction against corresponding bank
- 4 Refer to FBI PSA on Business Email Compromise Schemes
- 5 Financial Fraud Kill Chain for international wire transfers

## V. Working with partners

- How can you help real estate agents and other professionals you work with protect against wire fraud?

# Make sure they have 2FA enabled

- Make sure that real estate agents know that if they are using an unsecured e-mail address like gmail, they have enabled 2FA.



# Explain the benefits of a VPN

Share resources like this article from PCMag on the best VPN services for 2019.

<https://www.pcmag.com/roundup/296955/the-best-vpn-services>

Product	NordVPN	Private Internet Access VPN	ProtonVPN	TunnelBear VPN	CyberGhost VPN	ExpressVPN	IPVanish VPN	TorGuard VPN	Surfshark VPN	Symantec Norton Secure VPN
Lowest Price	SEE IT	SEE IT	SEE IT	SEE IT	SEE IT	SEE IT	SEE IT	SEE IT	SEE IT	SEE IT
Editors' Rating	★★★★★ EDITORS' CHOICE	★★★★☆ EDITORS' CHOICE	★★★★○ EDITORS' CHOICE	★★★★○ EDITORS' CHOICE	★★★★○	★★★★○	★★★★○	★★★★○	★★★★○	★★★★○
Best For	General Users	Power Users	Privacy Works	First-Time Users	General Users	Security Novices	General Users	Speedy BitTorrenting	Security Maximalists	Brand Loyalists
Supported Client Software	Android, Chrome, Firefox, iOS, Linux, macOS, Windows	Android, Chrome, Firefox, iOS, Linux, macOS, Windows	Android, iOS, macOS, Windows	Android, Chrome, iOS, macOS, Opera, Windows	Android, iOS, Linux, macOS, Windows	Android, iOS, Linux, macOS, Windows	Android, ChromeOS, iOS, Linux, macOS, Windows	Android, iOS, Linux, macOS, Windows	Android, Chrome, Firefox, FireTV, iOS, macOS, Windows	Android, iOS, macOS, Windows
Allows 5+ Simultaneous Connections	✓	✓	✓	✓	✓	—	✓	✓	✓	✓
500+ Servers	✓	✓	—	✓	✓	✓	✓	✓	✓	—
Geographically Diverse Servers	✓	✓	—	—	✓	✓	✓	✓	✓	✓
P2P or BitTorrent	✓	✓	✓	—	✓	✓	✓	✓	✓	—



# Educate Consumers

Most people don't notice these warnings in the email signature

“

**IMPORTANT NOTICE:** Never trust wiring instructions sent via email. Cyber criminals are hacking email accounts and sending emails with fake wiring instructions. These emails are convincing and sophisticated. Always independently confirm wiring instructions in person or via a telephone call to a trusted and verified phone number. Never wire money without double-checking that the wiring instructions are correct.

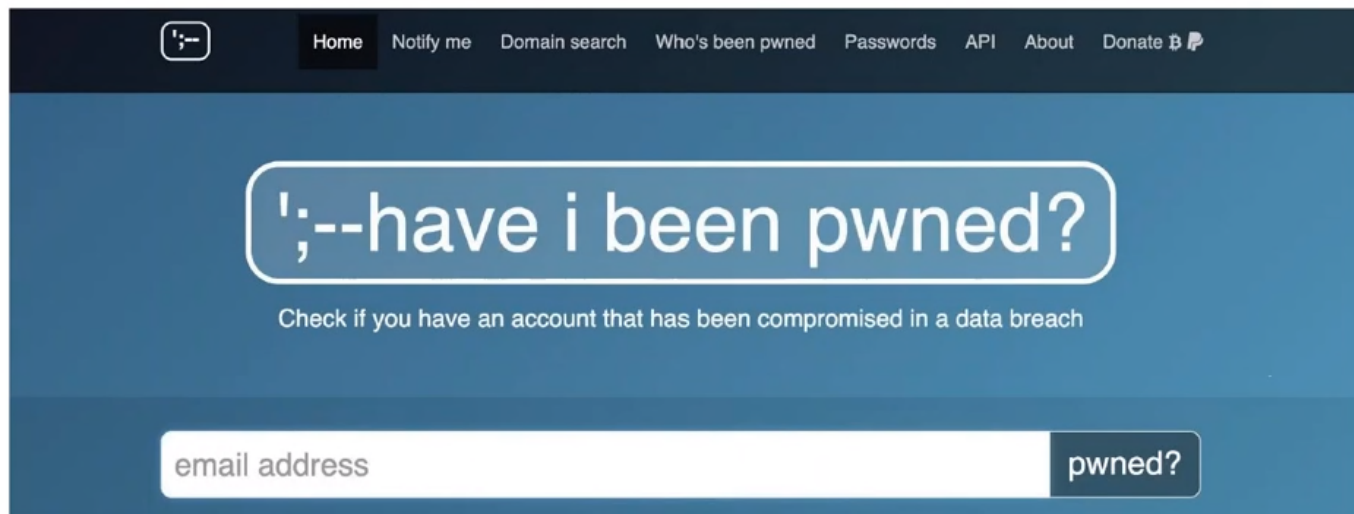
Share this video in the body of an email when communicating with a consumer.

[https://www.youtube.com/watch?time\\_continue=58&v=ek4TwC9owwY](https://www.youtube.com/watch?time_continue=58&v=ek4TwC9owwY)

[https://www.youtube.com/watch?time\\_continue=58&v=ek4TwC9owwY](https://www.youtube.com/watch?time_continue=58&v=ek4TwC9owwY)

# Have you been compromised?

Go to [haveibeenpwned.com](https://haveibeenpwned.com), if you have been “pwned” your email and possibly more information is at risk



The screenshot shows the homepage of haveibeenpwned.com. At the top, there is a dark navigation bar with a logo on the left and links for Home, Notify me, Domain search, Who's been pwned, Passwords, API, About, and Donate. The main content area has a blue background with a large white rounded rectangle containing the text "have i been pwned?". Below this, a smaller line of text says "Check if you have an account that has been compromised in a data breach". At the bottom, there is a white input field labeled "email address" and a dark button labeled "pwned?".

# Do you have cyber-liability insurance

- Even if you have such a policy, you must be following their guidelines before they will pay for a claim.

# Key Takeaways

## Hardware & Software

- Use strong passwords
- Encrypt your data
- Update hardware and software

## People & Process

- Be suspicious of email
- Train for prevention
- Conduct phishing tests

## Partners

- Work with like-minded
- Enable other real estate professionals
- Focus on education





**OLD REPUBLIC TITLE**

# Thank You!

