

# **Why Cyber Insurance is Non-Negotiable for the Title Industry**

A background image featuring a dark, starry night sky with a bright light source on the horizon, creating a silhouette of a sailboat on the water. The text is overlaid on this image.

**Joseph E. Brunsman, MSL**

**DISCLAIMER: The following is for general information purposes only. This presentation is not intended to provide official insurance or legal advice. Seek legal counsel familiar with your circumstances.**

**Many Thanks to:**



**OLD REPUBLIC TITLE**

---

A dark, hooded figure is seen from the chest up, looking through a circular opening. Inside the opening, a vibrant city skyline at night is visible, with numerous skyscrapers and lights. The scene is set against a solid black background.

# **What is Cyber Insurance?**

# Two Sides to Consider

## 3<sup>rd</sup> Party Coverage

**Your clients**

**Your vendors**

**Other parties**

**“Someone who wants  
money from your  
business”**

## 1<sup>st</sup> Party Coverage

**YOU**

**“Money your business  
has to - or needs to -  
pay”**



# Four Parts of 1<sup>st</sup> Party Cyber Insurance:

1. Data Breach & Cyber Events
2. Ransomware
3. *Loss of Funds (but not much)*
4. Miscellaneous

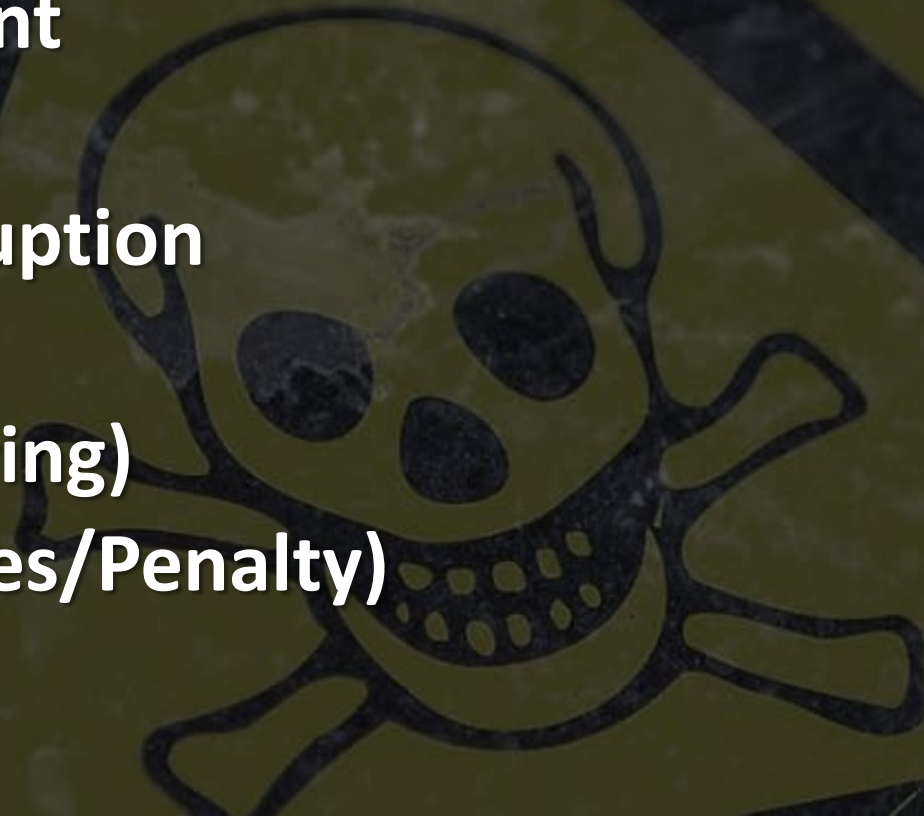


# Cyber Event (PII/PCI)

- Attorney
- Forensics
- Hacker Damage
- Notifications
- Credit Monitoring
- Business Int.

# Ransomware

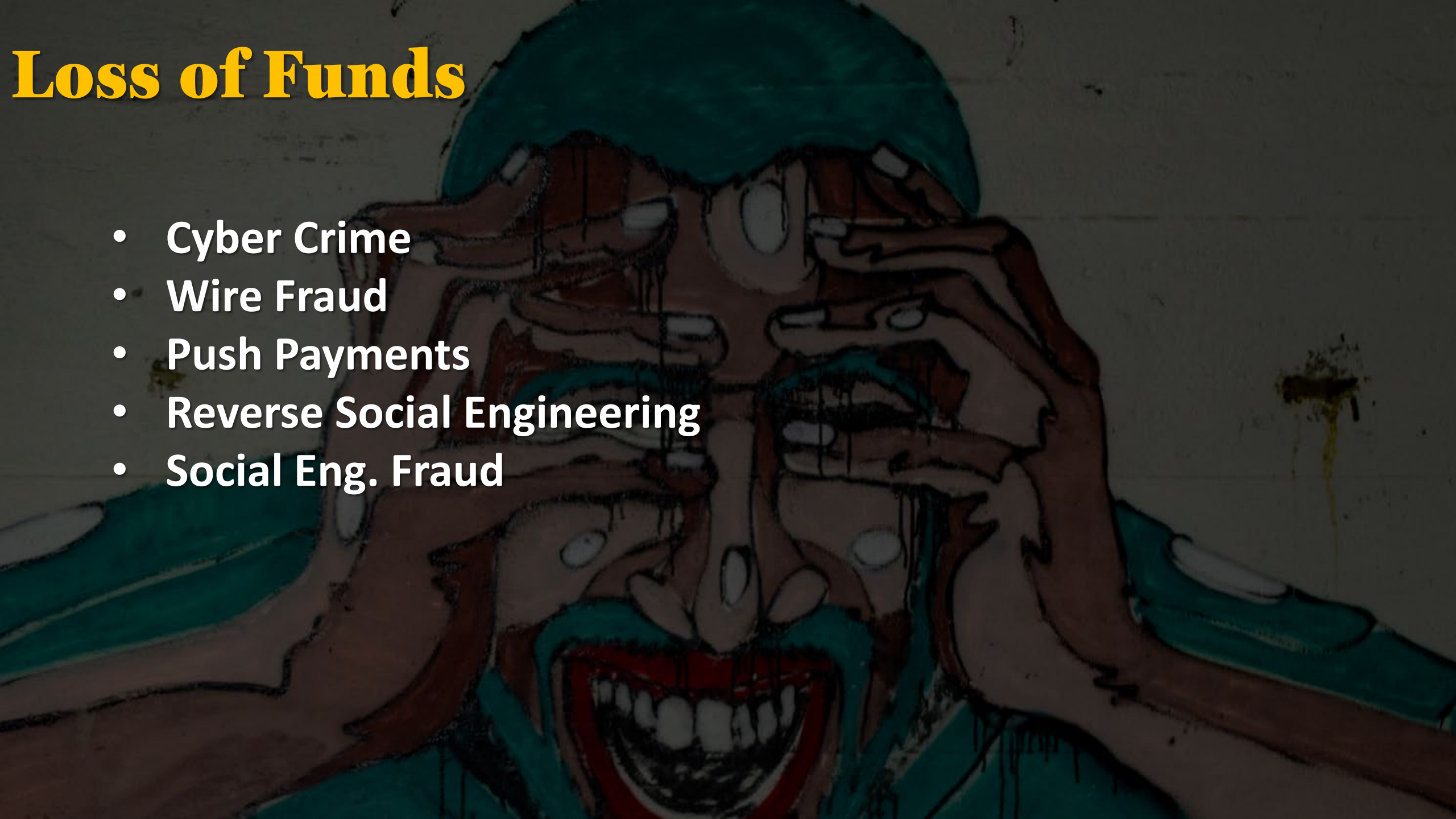
- Attorney
- Forensics
- Ransom Payment
- Hacker Damage
- Business Interruption
- (Notifications)
- (Credit Monitoring)
- (Regulatory Fines/Penalty)



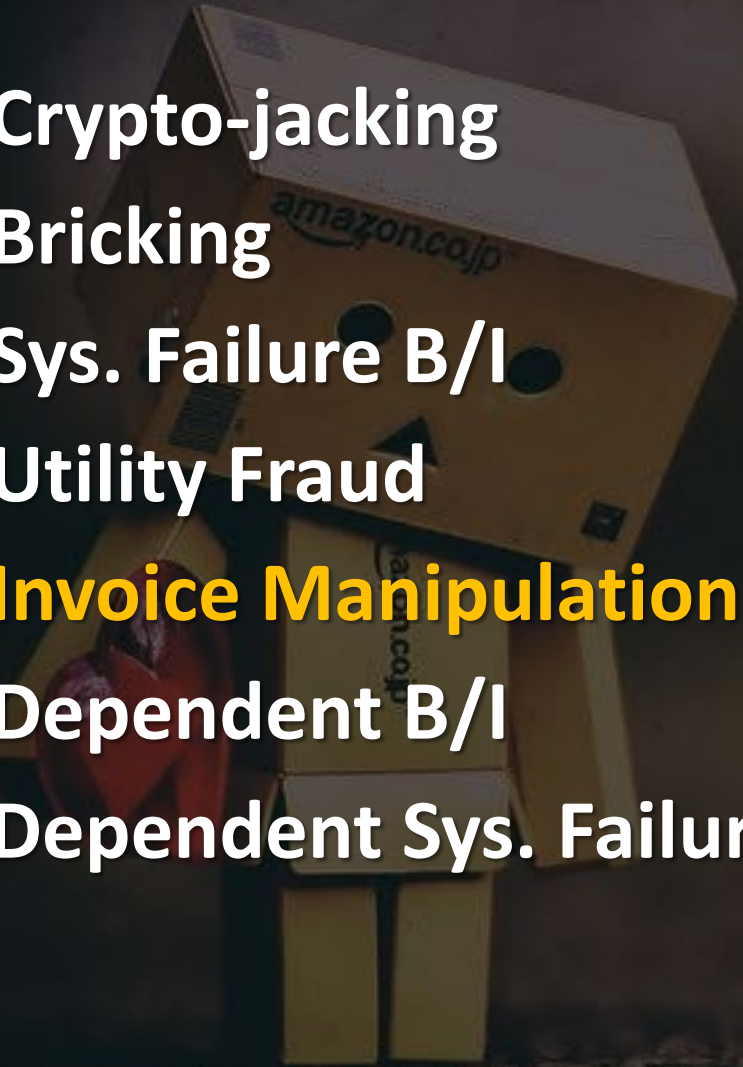


# Loss of Funds

- Cyber Crime
- Wire Fraud
- Push Payments
- Reverse Social Engineering
- Social Eng. Fraud



# Miscellaneous and Often Missing...

- 
- Crypto-jacking
  - Bricking
  - Sys. Failure B/I
  - Utility Fraud
  - **Invoice Manipulation**
  - Dependent B/I
  - Dependent Sys. Failure

- **Customers' Accounts**
- PCI/DSS
- Media Liability
- Vol. Shutdown
- BI/PD 1<sup>st</sup> and 3<sup>rd</sup> party
- Etc...



A person wearing a dark hoodie is shown from the chest up, looking through a circular opening in the fabric. The opening reveals a vibrant, blue-tinted city skyline at night, with numerous skyscrapers and lights reflecting on the water below. The text "Important Exclusions" is overlaid in a bold, yellow, serif font across the center of the image.

# **Important Exclusions**

# The Last 20 Years of Cyber Insurance

- Feel free to park your Ferrari in the Ghetto...
- Keep it running...
- Have no tracking device...
- Leave the bad guy a gift card in the console...
- Moving towards exclusions for “clean” declinations.

# Stricter Control Requirements

- What controls will my firm need?





# What if I've Heard Nothing So Far?

- My insurer hasn't demanded these yet.
- Insurers are starting to cut off specific industries, often at certain revenue thresholds.
- Ergo, you might not know until you'll need to scramble to implement controls.

# Broad Changes

- Caps on “Widespread” Events
- Co-insurance Requirements for Ransomware
- Lower limits and sub-limits (Cyber Crime & Ransomware)





# Critical Vulnerability Exclusions

## Critical Vulnerability Exclusion

- I. The following exclusion is added to the end of Section VI. Exclusions – What is not covered, A. Exclusions applicable to the entire Coverage Part:

- Critical vulnerability CV-1. based upon or arising out of any vulnerability exploitation within a **computer system**, program, network, application, operating system, software, firmware, or hardware, if:
- a. the vulnerability is recognized as a Common Vulnerability and Exposure (CVE) in the National Vulnerability Database operated by the National Institute of Standards and Technology and is assigned a base score or overall score of 8.0 or greater according to the latest version of the Common Vulnerability Scoring System (CVSS); and
  - b. a manufacturer or developer issued a patch to remedy such vulnerability and **you** failed to apply or deploy the issued patch within 14 calendar days of issuance.

# Old Hardware and Software Exclusions

## Unsupported or Legacy Computer Systems Exclusion

- II. The following exclusion is added to the end of Section VI. Exclusions – What is not covered, A. Exclusions applicable to the entire Coverage Part:

Unsupported/legacy computer systems UL-1. based upon or arising out of any vulnerability exploitation within a **computer system**, program, network, application, operating system, software, firmware, or hardware, if, as of the first known date of such vulnerability exploitation its developer or manufacturer has withdrawn or no longer supports such system, program, network, application, software, firmware, or hardware.

# “Monitoring” Remote Workers

- Electronic Communications Privacy Act + Others.

## Exclude Wrongful Capture and Use of Data

III. The following exclusion is added to the end of Section VI. Exclusions – What is not covered, A. Exclusions applicable to the entire Coverage Part:

Wrongful capture  
and use of data

WC-1. based upon or arising out of any actual or alleged monitoring, tracking, or profiling of an individual, without that individual’s authorization, including but not limited to web-tracking, session recording, digital fingerprinting, behavioral monitoring, eavesdropping, wiretapping, audio or video recording, and use of any data resulting from such activities by **you** or by a third party on **your** behalf with **your** knowledge and consent.

# “Zero Day” Exclusions

## Zero Day Attacks Exclusion

- I. The following exclusion is added to the end of Section VI. Exclusions – What is not covered, A. Exclusions applicable to the entire Coverage Part:  

Zero day attacks	ZD-A. based upon or arising out of the use of any vulnerability or zero day exploitation within a program, application, operating system, software, firmware, or hardware either before the developer or manufacturer has issued a patch or within seven days of such a patch being issued.
------------------	---





## ECONOMIC AND TRADE SANCTIONS POLICYHOLDER NOTICE

---

Hiscox is committed to complying with the U.S. Department of Treasury **Office of Foreign Assets Control (OFAC)** requirements. OFAC administers and enforces economic sanctions policy based on Presidential declarations of national emergency. OFAC has identified and listed numerous foreign agents, front organizations, terrorists, and narcotics traffickers as Specially Designated Nationals (SDN's) and Blocked Persons. OFAC has also identified Sanctioned Countries. A list of Specially Designated Nationals, Blocked Persons and Sanctioned Countries may be found on the United States Treasury's web site <http://www.treas.gov/offices/enforcement/ofac/>.

Economic sanctions prohibit all United States citizens (including corporations and other entities) and permanent resident aliens from engaging in transactions with Specially Designated Nationals, Blocked Persons and Sanctioned Countries. Hiscox may not accept premium from or issue a policy to insure property of or make a claim payment to a Specially Designated National or Blocked Person. **Hiscox may not engage in business transactions with a Sanctioned Country.**





A dark, atmospheric tunnel with walls covered in graffiti. In the center, a large, glowing neon letter 'P' is illuminated with a warm, orange-red light. The text 'Poll Question #1' is overlaid in a bold, yellow, serif font across the middle of the image.

# **Poll Question #1**

A dark, hooded figure is shown from the chest up, with the hood pulled over their head. The figure is looking through a circular opening, which reveals a brightly lit city skyline at night. The city lights are reflected in the water in the foreground. The overall mood is mysterious and somewhat ominous.

# **FTC Safeguards Rule**

# The Safeguards Rule

- The requirements are not a, “check list.”
- Enforcement is *Brutal and Personal*.
- Cyber Insurance probably won't pay for this.
- Interpretations will change, so keep up.



# Prior FTC Action...

## Real Estate Services Company Settles Privacy and Security Charge

Company Tossed Consumers' Confidential Information in Dumpster; Company Computers Were Hacked

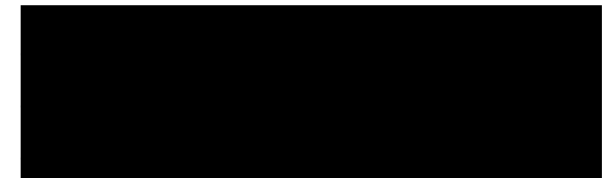
May 10, 2006



**Tags:** [Consumer Protection](#) | [Privacy and Security](#) | [Data Security](#)

A title company that promised consumers it maintained "physical, electronic and procedural safeguards" to protect their confidential financial information, but tossed consumer home loan applications in an open dumpster, agreed to settle Federal Trade Commission charges that its inadequate storage and disposal procedures for sensitive consumer information violated federal laws. The settlement with [REDACTED] Title Agency, Inc., [REDACTED] Holding Company, and [REDACTED] bars deceptive claims about privacy and security policies, and requires that they implement a comprehensive information security program and obtain audits by an independent third-party security professional every other year for 20 years.

### Related Cases



### Topics

[Privacy and Security Enforcement](#)

# What Types of Information Do You Hold?

1. Driver's License, Passport, Social Security Numbers, etc.
2. Bank Information such as: Bank Name, Bank Address, Routing Number, Account Numbers, Etc.
3. Tax Information, Tax Assessments, Outstanding Liens or Taxes, Etc.
4. Loan Information, Etc.

*How long are you holding that data, and what is a record?*



# Who Shall Adhere?

- “An entity is a financial institutions if it’s engaged in an activity that is financial in nature or is incidental to such activities....”
- Per the FTC: *“what matters are the types of activities your business undertakes, not how you or others categorize your company.”*

# Who is Wholly Exempt?

- Certain Institutions chartered by Congress.
- “Entities that engage in financial activities but that are not significantly engaged in those financial activities, and entities that engage in activities incidental to financial activities but that are not significantly engaged in activities incidental to financial activities.”
- What does that mean?
- *It means: ask the attorney!*

# What Are You Safeguarding?

- **Customer Information** – “means any record containing **nonpublic personal information** about a customer of a financial institution, whether in paper, electronic, or other form, that is handled or maintained by or on behalf of you or your affiliates.”
- **Nonpublic Personal Information** – “(i) Personally identifiable financial information; and (ii) Any list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived using any personally identifiable financial information that is not publicly available.”

# How Do You Safeguard That Data?

- Written Information Security Program appropriate to the size and complexity of your business, your activities, and the information you hold.
- Encompasses: Administrative, Physical, and Technical Safeguards.
- Ergo, the program must be, “*reasonable.*”



# Continued

- Designate a “Qualified Individual” to implement and supervise the Security Program. (CIO/VCIO)
- Conduct periodic Risk Assessments. (Exemption)
- Implement and review access controls.
- Inventory data and devices.
- Encrypt customer information while resting & in transit.
- Assess the security of your applications.
- Implement MFA for anyone accessing customer information.

# There's More

- Dispose of customer info securely after 2 years unless needed.
- Anticipate and evaluate changes to your system/network. “Your Safeguards can’t be static” (POI)
- Log of authorized/un-authorized user access.
- Continuous monitoring or: Annual Pen testing and Vuln Assessments, including system wide scans every six months. (Exemption)
- Security awareness training for employees is *mandatory*.
- Monitor Service Providers. Example: *MSP QBRs*.
- Create a written incident response plan. Which includes:  
“A process to fix any identified weaknesses in your systems and controls.” (POI) (Exemption)



# About that Qualified Individual

Regardless of firm size, you still have to appoint a Qualified Individual to oversee the program.

If you have over 5,000 consumer records the Qualified Individual must report:

- Overall status of the info sec program and your compliance status.

- Address the risk assessment, risk management and control decisions, service provider arrangements, results of testing, security events or violations and management's response, and recommended changes.



# Continued...

Directly from the FTC regarding “Qualified Individual”

“If your company brings in a service provider to implement and supervise your program, **the buck still stops with you.**”

“It’s your company’s responsibility to designate a senior employee to supervise that person.”

“If the Qualified Individual works for an affiliate or service provider, that affiliate or service provider also must maintain an information security program that protects your business.”



A dark, atmospheric tunnel with walls covered in graffiti. In the center, a large, glowing neon letter 'P' is illuminated with a warm, orange-red light. The text 'Poll Question #2' is overlaid in a bold, yellow font across the middle of the image.

# **Poll Question #2**

# Enforcement

- Eight different federal agencies can enforce this rule.
- Could deal with:

1. **Company Enforcement**

<https://www.ftc.gov/enforcement/cases-proceedings/terms/1420>

2. ***Individual Enforcement***



# Company Enforcement

- *In the Matter of Gregory Navone*
- By the time of the FTC action, most of his companies were either no longer operational or were being operated by someone else.



[illegible]

## X. Order Effective Date

**IT IS FURTHER ORDERED** that this Order is final and effective upon the date of its publication on the Commission's website (E-Reg.gov) as a final order. This Order will become binding (20 years) from the date of its publication (which date may be extended at the end of this Order upon the Commission's finding) or twenty (20) years from the most recent date that the United States or the Commission takes a compliance action or inaction, as appropriate (not to exceed) in Federal court alleging any violation of this Order, whichever occurs later; provided, however, that the filing of such a complaint will not affect the character of:

- A. Any President in this Order that is under 18 years of age;
- B. This Order's application to any Respondent that is not named as a defendant in such complaint; and
- C. This Order if such complaint is filed after the Order has terminated pursuant to this Provision.

**Provided, further,** that if such complaint is dismissed or a federal court rules that the Respondent did not violate any Provision of the Order, and the dismissal or ruling is either not appealed or upheld on appeal, then the Order will not transmit according to this Provision as though the complaint had never been filed, except that the Order will not transmit between the date such complaint is filed and the date of the deadline for appealing such dismissal or ruling and the date such dismissal or ruling is upheld on appeal.

By the Contributors

R. J. Taylor

SEAL  
ENCLOSURE December 30, 2011

<https://www.ftc.gov/datasecurity>

**Create WISP**  
**Essentially Create CISO**  
**Risk Assessments**  
**Doc. Retention & Destruction**  
**Code Reviews**  
**Pen. Testing**  
**Input Validations**  
**Network Segmentation**  
**IPDS Implementation**  
**File Integrity Monitoring Tools**  
**Data Loss Prevention Tools**  
**Location Upload Restrictions**  
**Encryption of PII**  
**Vulnerability Testing**  
**Service Provider Selection...**  
**Yearly Certification to FTC**  
**Compliance Reports**  
**Accounting Record Issues**  
**Employee Training**  
**FOR 20 YEARS....**



# Leadership Enforcement

**Government Now  
Holds CEOs  
*Personally Responsible*  
for Data Security**

**Joseph E. Brunsman, MSL**

DISCLAIMER: The following is for general information purposes only. This presentation is not intended to provide official insurance or legal advice. Seek legal counsel familiar with your circumstances.

# Does Cyber Insurance Cover This?

## Common policy exclusions:

- “costs to establish or improve security or privacy practices; or audit, reporting, or compliance costs.”



# State Level Exemptions?

- GLBA generally preempts state laws only to the extent that they are conflicting.
- GLBA does *not* preempt state laws which are more protective.
- Many states have consumer protection laws which are stricter.

## Examples:

1. If you have Massachusetts clients; 201 CMR 17.
2. If you fall under NYDFS; 23 NYCRR 500.

# XYZ Title Insurance Company

- SEC Settlement: ~\$490k Civil Penalty.
- NYDFS 23NYCRR500: Filed charges in July of 2020 – *ongoing*
  - Failed to follow its own policies.
  - Neglected to conduct a Security Review and Risk Assessment.
  - Misclassified the vulnerability.
  - Failed to investigate IAW its own internal cybersecurity policies.
  - *Failed to follow the recommendations of its own security team...*



## Recent Company

# Data Breach Alert: [REDACTED] Title & Escrow, LLC

---

NOTICE: If you received a NOTICE OF DATA BREACH letter from [REDACTED] Title & Escrow, contact the attorneys at Console & Associates at [\(866\) 778-5500](tel:(866)778-5500) to discuss your legal options, or submit a confidential Case Evaluation form [here](#).

# Even a Hint of A Breach....

RE: Notice of Data Breach

Dear [REDACTED]

[REDACTED] Title Insurance Company [REDACTED], is writing to advise you of a recent event that may impact the security of certain personal information related to you. We write to provide you with information about the event, steps taken since discovering the event, and what you can do to better protect against potential misuse of your information, should you feel it is appropriate to do so.

***What Happened?*** On January 12, 2020, [REDACTED] became aware of unusual activity on its network. [REDACTED] conducted an immediate investigation and determined that the network was partially impacted by malware. Third-party forensic investigators were engaged to assist in the investigation to determine the nature and scope of the event, and identify what personal information may have been impacted by this event.

Through the investigation, [REDACTED] identified a database containing sensitive information that was accessed by the unauthorized individual(s) during this event. The database contained individuals' names and certain data relating to those individuals. However, the names were not easily associated with the data relating to those individuals. To match the individual with any associated data, particular tools and a specialized understanding of the database is required. As such, [REDACTED] began an extensive review of its records to properly identify the addresses and associated data for the affected individuals. This review concluded on July 10, 2020.

***What Information Was Involved?*** The following information about you was included in the impacted database: your name, EXTRA1 ITEM1, ITEM2, ETC. While the data relating to you was not readily associated with your name, we are notifying you out of an abundance of caution.

***What We Are Doing.*** [REDACTED] is committed to, and takes very seriously, its responsibility to protect all data entrusted to us. As part of our ongoing commitment to the privacy of personal information in our care, we reviewed our existing policies and procedures, and are working to implement additional safeguards to further secure the information contained within our network. [REDACTED] is also notifying regulatory authorities, as required by law.

# Again....

Turke & Strauss LLP, a leading data breach law firm, is investigating [REDACTED] which does business as [REDACTED] Title Company and [REDACTED], regarding its recent data breach. The [REDACTED] Title Company data breach involved sensitive personal identifiable information belonging to over 1,250 individuals.

## ABOUT [REDACTED] TITLE COMPANY:

[REDACTED] Title Company is an insurance and closing service provider that has been serving [REDACTED]. As a home and property insurance company, [REDACTED] Title Company offers a variety of services from complete closing services, short sale closings, and full title insurance, to Title examination and construction loan closings. Headquartered in [REDACTED] Title Company has locations in [REDACTED]

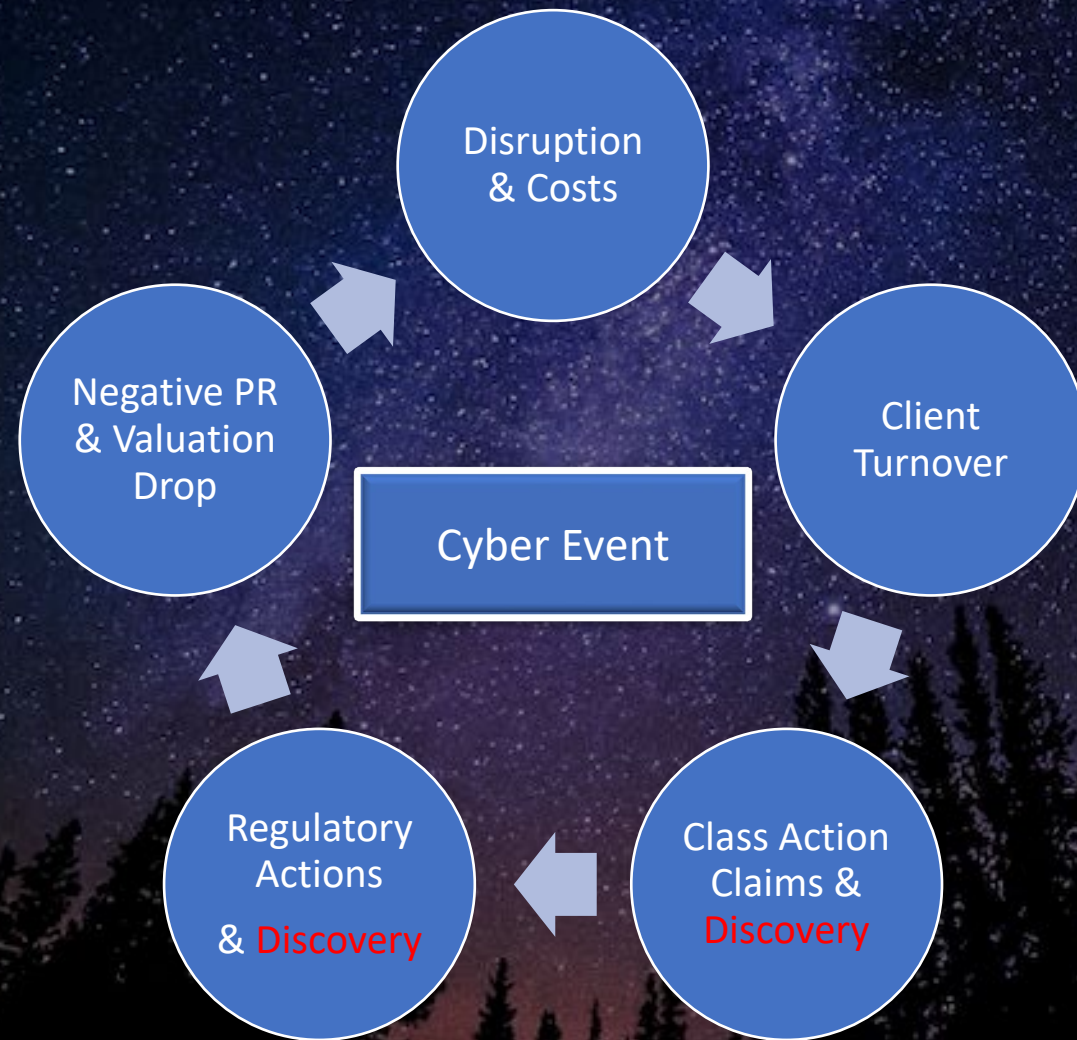
## WHAT HAPPENED?

On November 18, 2022, [REDACTED] Title Company discovered that it had experienced a data breach in which the sensitive personal identifiable information in its systems may have been accessed. Through its investigation, [REDACTED] Title Company determined that an unauthorized actor may have accessed this sensitive information on November 18, 2022. On April 4, 2023, [REDACTED] Title Company began contacting individuals whose information may have been impacted. The type of information exposed includes:

- Name
- Social Security number
- Driver's license
- Financial account numbers



# Beware the Data Breach Death Spiral





# Take-Aways

- You *will* increase your security: The Easy Way, or, The Hard Way.
- Get a baseline “record” count.
- Investigate your legal obligations.
- Work on a Plan of Implementation & follow it.
- WISPs are unique to your business & will be scrutinized.
- *Please* read your cyber insurance policy & ask questions!
- You may require a VCIO...