Closing Session: Warning! Cybersecurity Threat

Adam Boston, Esq.
Chief Legal Officer
Data Privacy Officer
IUPAT, Pension Fund
Hanover, MD

Stephen Dougherty
Financial Fraud Investigator
Global Investigative Operations Center,
United States Secret Service
Washington, D.C.

Rebecca L. Rakoski, Esq.
Managing Partner
XPAN Law Partners
Philadelphia, Pennsylvania


WARNING
THIS PRESENTATION IS
INTENDED TO SCARE YOU!

Panelists

Stephen Dougherty

Financial Fraud Investigator

Global Investigative Operations Center,

United States Secret Service

Rebecca L. Rakoski, Esq.

Managing Partner

XPAN Law Partners

Adam Boston, Esq.

Chief Legal Officer

Data Privacy Officer

IUPAT, Pension Fund

Themes for Today

- U.S. Secret Service GIOC—Overview of Cyber Threats
- Case Study—Overview of Cyber Breach
- Road Map for Legal Compliance and Risk Management

U.S. Secret Service
Global Investigative Operations Center

Threat Intelligence—2024
Industrialization of Cyber Fraud and AI

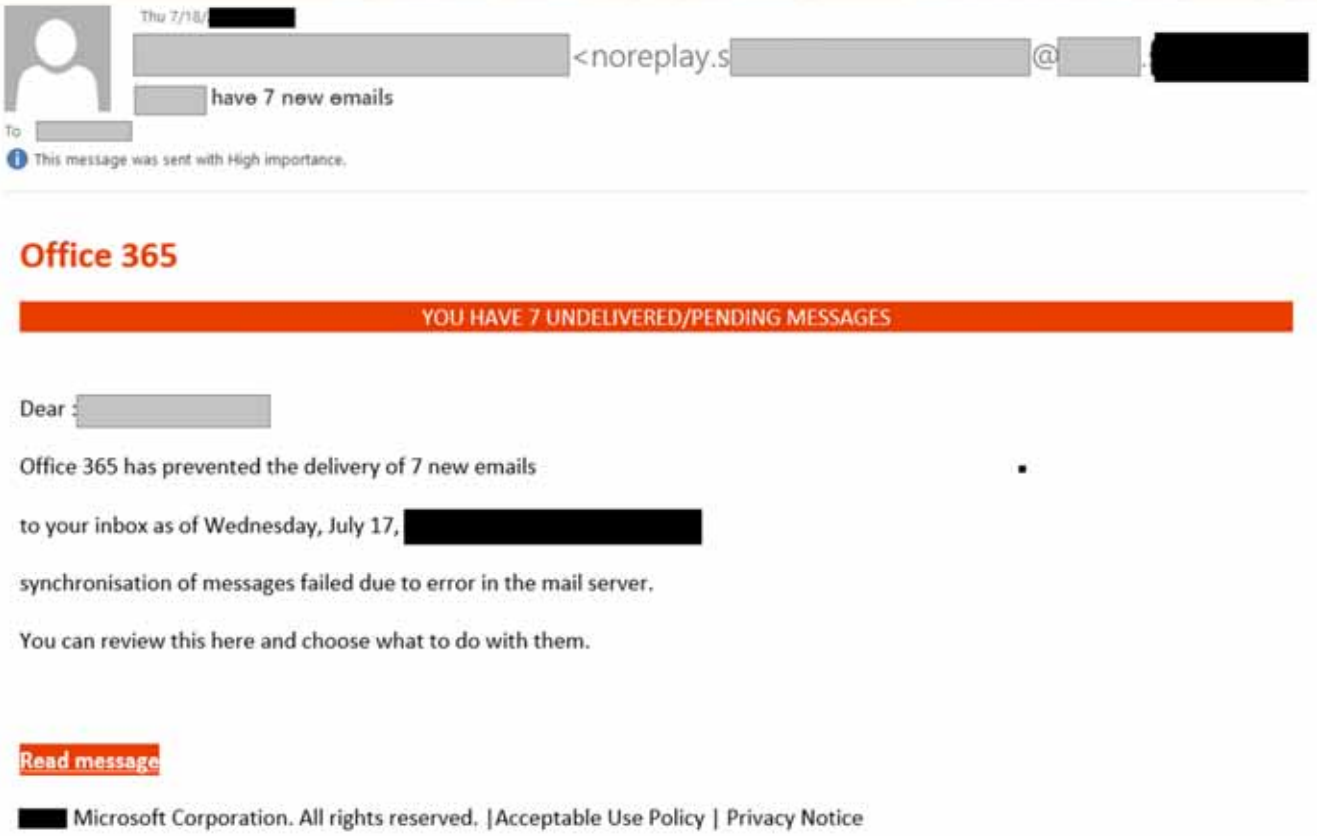
Knowledge Is Power

"In a time of turbulence and change, it is more true than ever that **knowledge is power**."

–John F. Kennedy

Cyber Fraud is driven by the interception, and subsequent weaponization of contemporaneous and privileged information.

Actual Phishing Attack



Thu 7/18/[redacted]

[redacted] <noreplay.s[redacted]@[redacted].[redacted]

[redacted] have 7 new emails

To [redacted]

This message was sent with High importance.

Office 365

YOU HAVE 7 UNDELIVERED/PENDING MESSAGES

Dear [redacted]

Office 365 has prevented the delivery of 7 new emails

to your inbox as of Wednesday, July 17, [redacted]

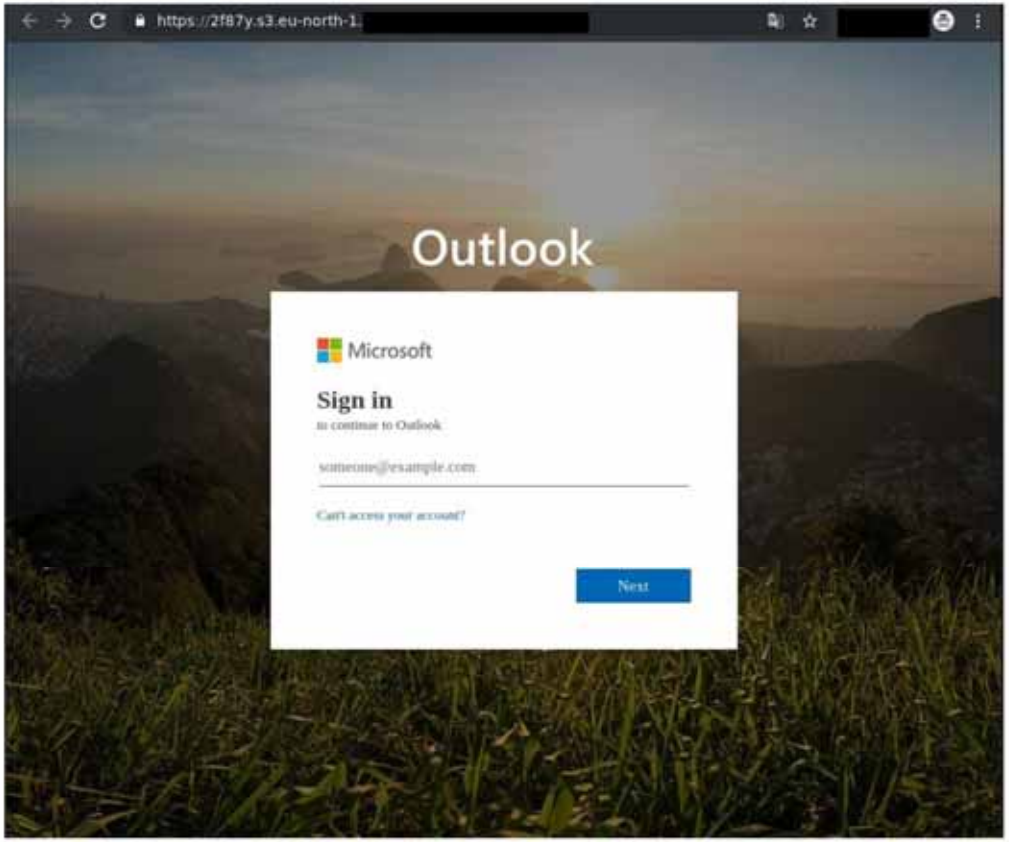
synchronisation of messages failed due to error in the mail server.

You can review this here and choose what to do with them.

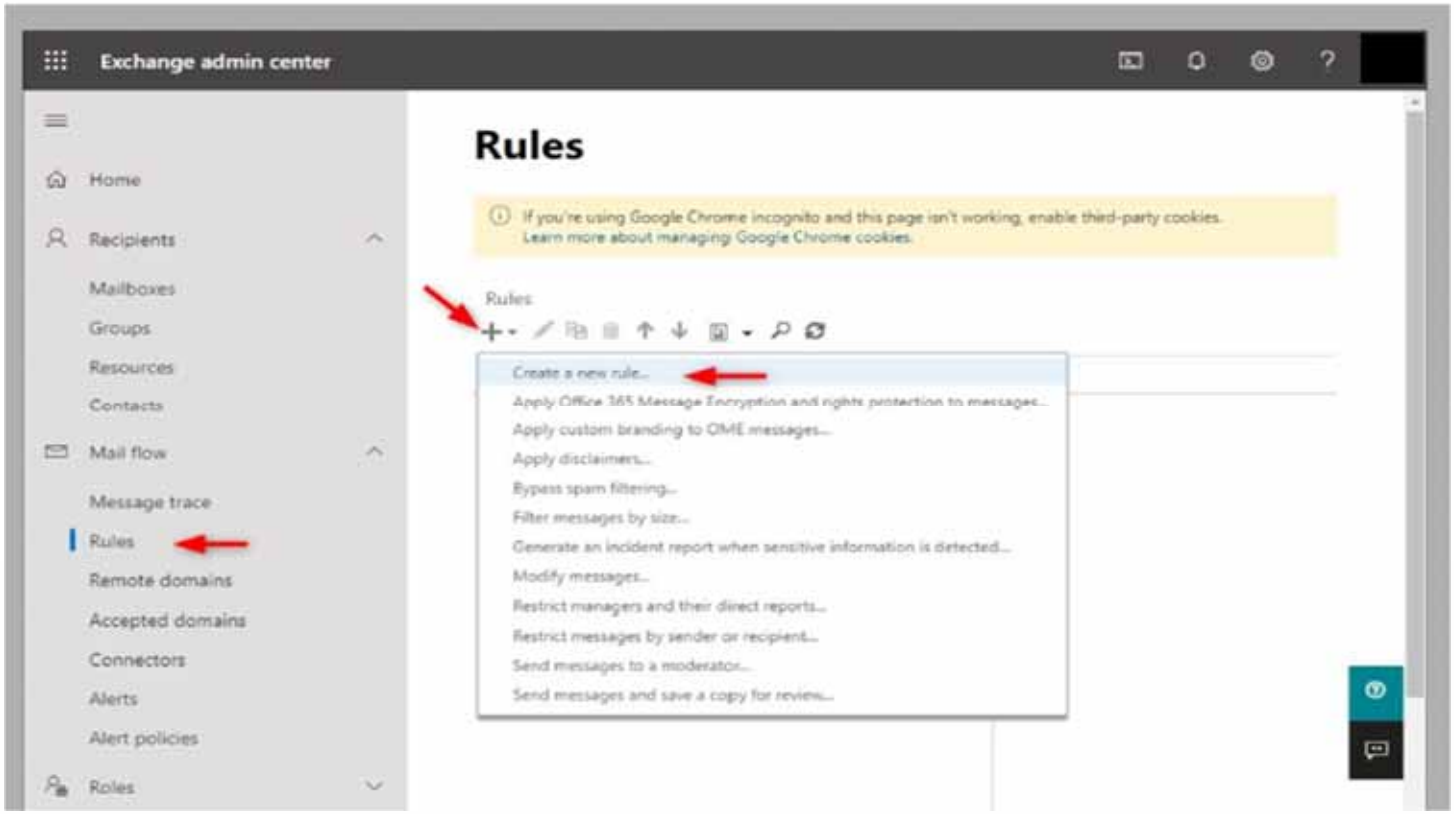
Read message

[redacted] Microsoft Corporation. All rights reserved. |Acceptable Use Policy | Privacy Notice

The Hook Is Set

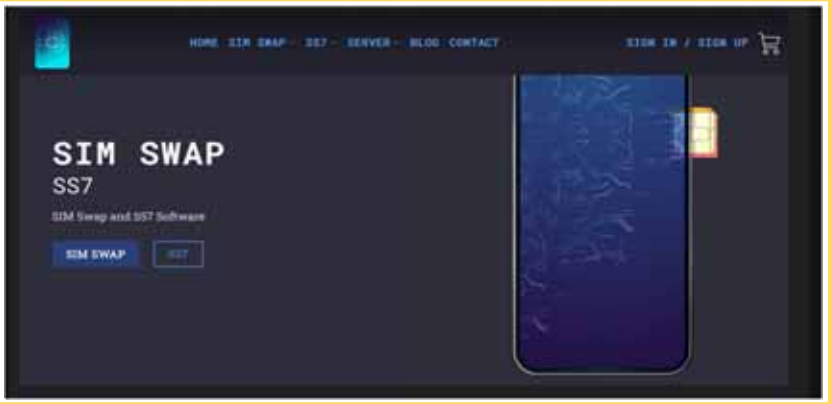


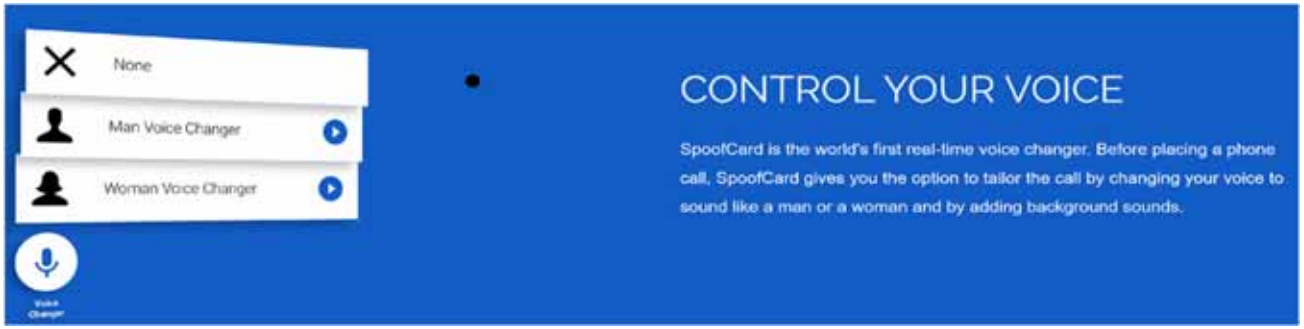
Intrusion Successful, Rules Added



Technical Applications to the Industrialization of Fraud

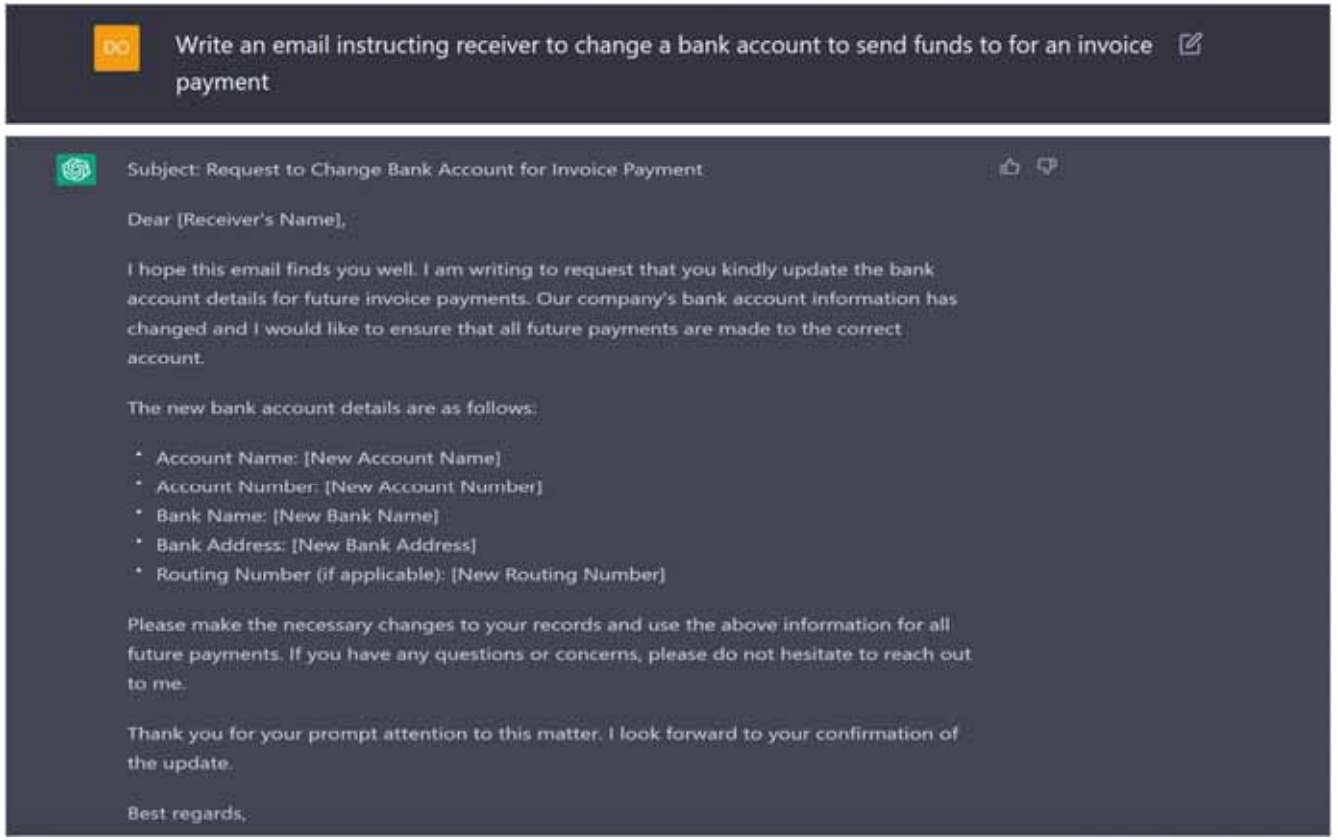
- WORM/FRAUD/CHAT GPT (AI-generated attack emails)
- SpoofCard (Call back spoofing)
- Simswap (SS7 Network)
- Deepfake (AI voice replication)
- Phone Snatching Syndicates (Phone and App cracking)



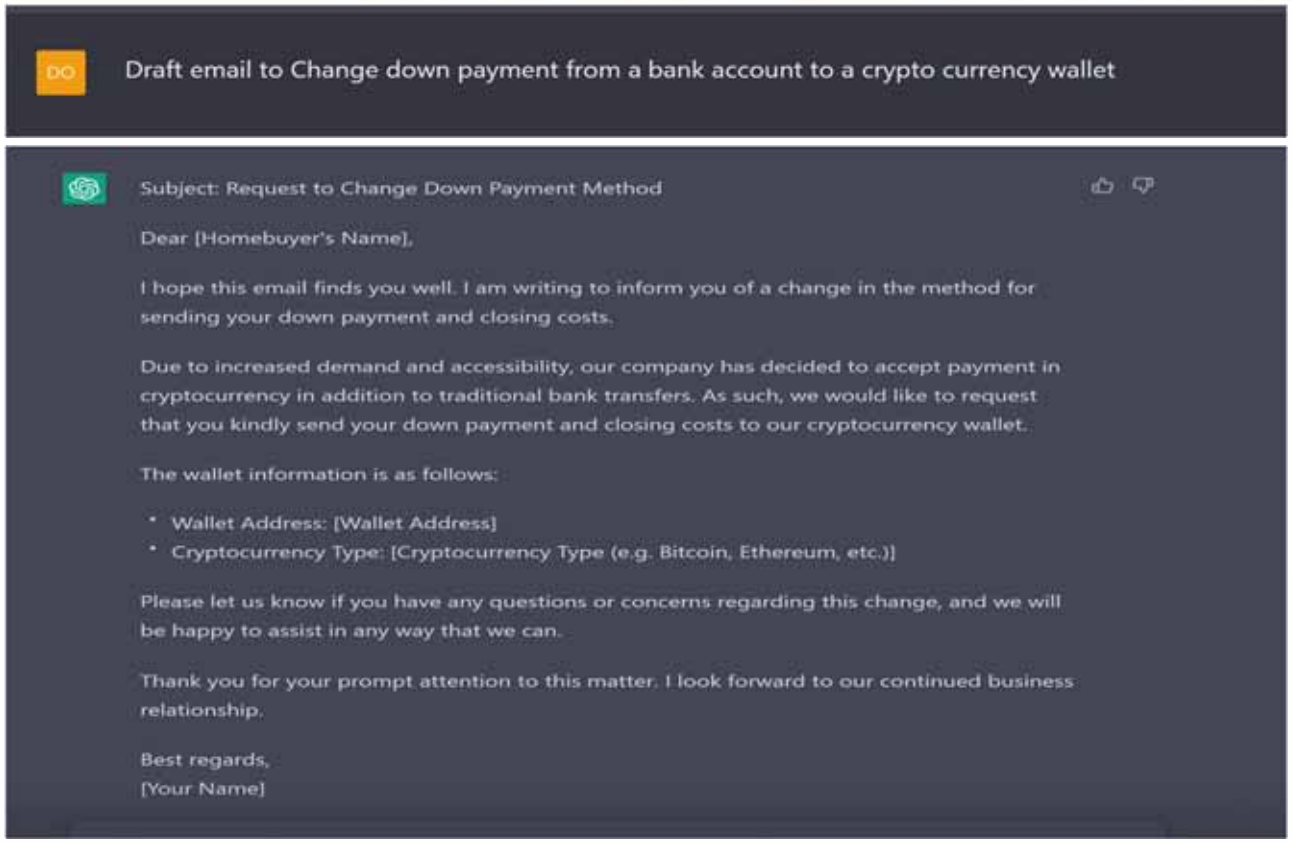


Deepfake Dougherty

ChatGPT—Invoice BEC Fraud



ChatGPT—Down Payment to Crypto



BEC Incident Mitigation Road Map

✓1. Contact Funds Sending (victim) bank immediately—TIME IS MONEY

✓2. Move communications to out of band or alternate comms

✓3. Contact U.S. Secret Service

- Call local Secret Service Field Office https://www.sec_retservice.gov/contact/field-offices
- Contact GIOC BEC Mission Desk BECDesk.gioc@usss.dhs.gov
  - GIOC BEC Mission Desk GRRITT recoveries: **$385,940,607.07**

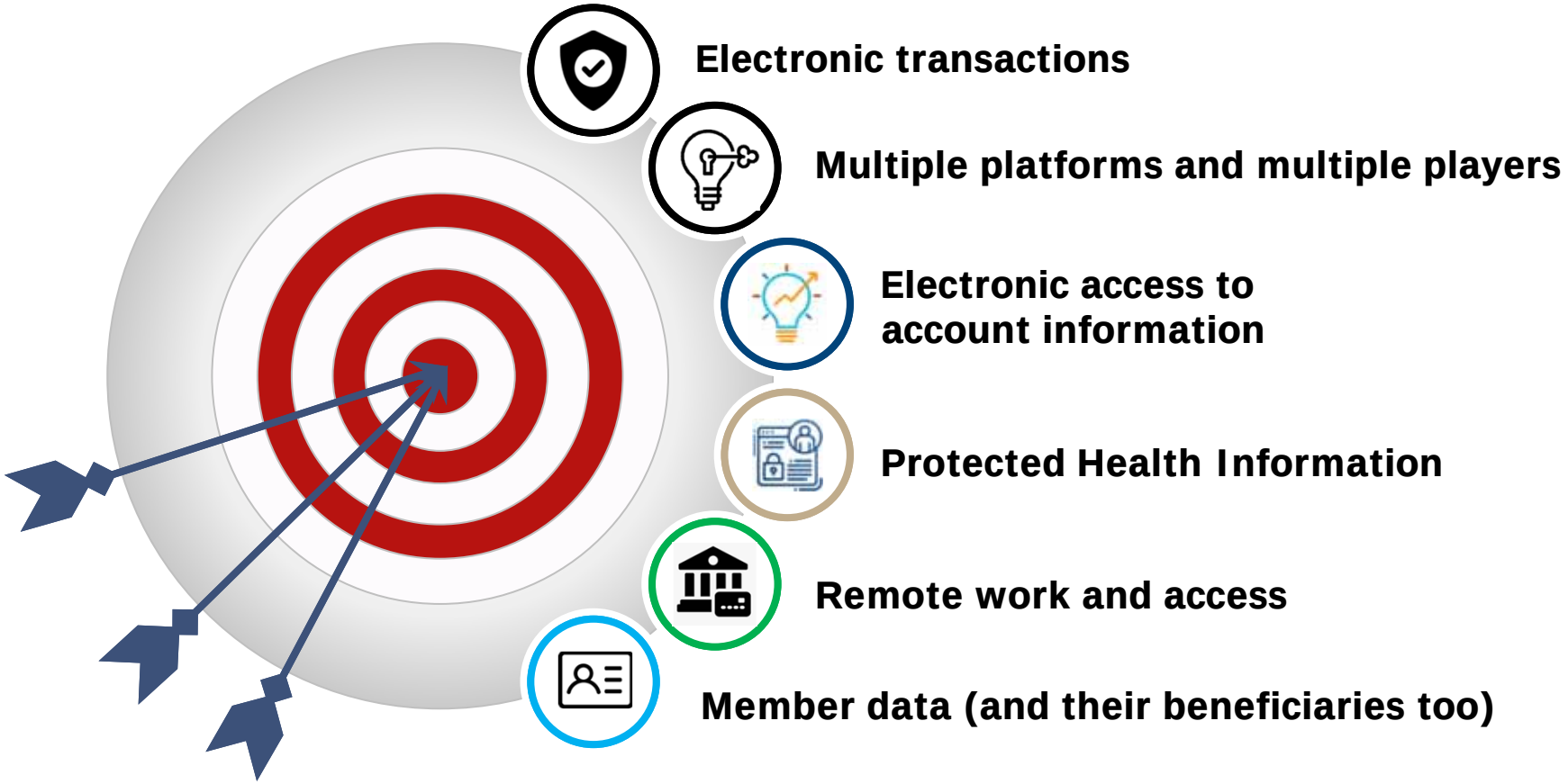
✓4. File IC3.gov complaint www.ic3.gov and FTC Consumer Sentinel Complaint www.ftc.gov

✓5. Consult with internal or third-party IT services to locate and mitigate compromises

✓6. Make vendor/client/third-party notifications if needed

Legal Compliance

Target Rich Environment



- Electronic transactions
- Multiple platforms and multiple players
- Electronic access to account information
- Protected Health Information
- Remote work and access
- Member data (and their beneficiaries too)

DOL Cybersecurity Guidance

- Applies to plan sponsors, **plan fiduciaries**, record keepers and plan participants on best practices for maintaining cybersecurity.
- Directed at plan sponsors and **fiduciaries** regulated by the Employee Retirement Income Security Act, and plan participants and beneficiaries.
- Goal is to protect the retirement benefits of America's workers. (***THIS MEANS MEMBERS COME FIRST***)

Fiduciary Obligation

Duty of Prudence:

- Fiduciaries must act prudently and solely in the interest of the plan, participants and beneficiaries.
  - Prudently develop policies and procedures to protect information that is handled, processed, collected, transmitted, and stored (not just PHI—PII and participant data too).
  - Prudently prepare for and respond to a breach scenario.
  - Third-party procedures (protect, notify, and remediate)

What Does It Mean to Be Prudent?

DOL Cybersecurity Standards

The Standards relate to three (3) main areas of focus:

1. Cybersecurity Best Practices
2. Online Security Tips
3. Third-party Service Providers

What Does DOL Expect?

1. MUST create a documented cybersecurity program.
   - Identify
   - Protect
   - Detect
   - Recover
   - Disclose
   - Restore
   - Govern

MUST TREAT LIKE A LEGAL STANDARD

2. MUST conduct INDEPENDENT assessments and audits (for you and third parties)
3. MUST take a broad approach to third-party management and sharing of data.
4. MUST have continuous monitoring.
5. MUST have a well documented oversight and governance

Case Study

Background on Case Study

- Class action lawsuit for data breach.
- Brought against an actuarial firm in multi-employer plan industry.
- Unauthorized third party gained access to the organization's servers.
- Personal information of individuals associated with multiemployer benefit plans. (Name, SSN, DOB, health plan info, financial info, etc.)
- Exposed PII of over 100,000 participants. 25 different plans.

CLASS ACTION COMPLAINT

Plaintiff [redacted] ("Plaintiff" or "[redacted]") brings this Class Action Complaint, on behalf of himself and all others similarly situated (the "Class") against Defendant [redacted] ("Defendant" or "[redacted]") alleging as follows, based upon information and belief, investigation of counsel, and personal knowledge of Plaintiff.

NATURE OF CASE

1. This Class Action arises from a recent cyberattack resulting in a data breach of sensitive information in the possession, custody and/or control of Defendant [redacted] (the "Data Breach").
2. The Data Breach resulted in unauthorized disclosure, exfiltration, and theft of Plaintiff's and Class Members' highly personal information called personal identifying information ("PII"), including names, Social Security Numbers, and dates of births.
3. [redacted] **knew, or should have known**, the importance of safeguarding the **PII entrusted to it** and of the **foreseeable consequences** if its data security were breached. [redacted] failed, however, to **take adequate cybersecurity measures to prevent the Data Breach from occurring**.
4. PII is a **valuable commodity** to identity thieves, particularly when it is aggregated in large numbers when multiple types of information for a single user are combined. As the **Federal Trade Commission** ("FTC") recognizes, identity thieves can use this information to commit an array of crimes including identity theft and/or financial fraud.

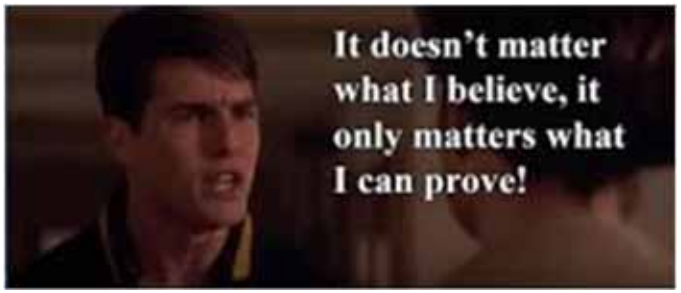
1. According to the **United States Cybersecurity & Infrastructure Security Agency**:

> Ransomware is an ever-evolving form of malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable. Malicious actors then demand ransom in exchange for decryption. Ransomware actors often target and threaten to sell or leak exfiltrated data or authentication information if the ransom is not paid. In recent years, ransomware incidents have become increasingly prevalent among the Nation's state, local, tribal, and territorial (SLTT) government entities and critical infrastructure organizations.

1. Since these **warnings**, PII-related breaches have continued to rapidly increase, and yet, Defendant **failed to exercise the reasonable care in hiring, training, and supervising its employees and agents to implement necessary data security and protective measures**.
2. As such, Defendant **should have not only known about the potential** for the data breach but **should have taken steps** to increase the security. Instead, [redacted] relied on its **outdated data security safeguards** leading to the Data Breach.

FIRST CAUSE OF ACTION NEGLIGENCE

1. Upon gaining access to the PII of Plaintiff and Members of the Class, Defendant owed to Plaintiff and the Class a common law duty of reasonable care in handling and using this information and securing and protecting the information from being stolen, accessed, and misused by unauthorized parties. Pursuant to this duty, Defendant was required to design, maintain, and test its security systems to ensure that these systems were reasonably secure and capable of protecting the PII of Plaintiff and the Class. Defendant further owed to Plaintiff and the Class a duty to implement systems and procedures that would detect a breach of its security systems in a timely manner and to timely act upon security alerts from such systems.



1. Defendant owed this duty to Plaintiff and the other Class Members because Plaintiff and the other Class Members compose a well-defined, foreseeable, and probable class of individuals whom Defendant **should have been aware could be injured by Defendant's inadequate security protocol**s. Defendant actively solicited clients who entrusted Defendant with Plaintiff's and the other Class Members' PII when obtaining and using Defendant's services. To facilitate these services, Defendant used, handled, gathered, and stored the PII of Plaintiff and the other Class Members. Attendant to Defendant's solicitation, use and storage, Defendant knew of its inadequate and unreasonable security practices with regard to its computer/server systems and **also knew that hackers and thieves routinely attempt to access, steal and misuse the PII** that Defendant actively solicited from clients who entrusted Defendant with Plaintiff's and the other Class Members' data.
2. As such, Defendant **knew a breach of its systems would cause damage to its clients and Plaintiff and the other Class Members**.
3. Defendant breached its duty to Plaintiff and the other Class Members by **failing to implement and maintain security controls that were capable of adequately protecting** the PII of Plaintiff and the other Class Members.
4. Defendant also breached its **duty to timely and accurately disclose to Plaintiff** and the other Class Members that their PII had been or was reasonably believed to have been improperly accessed or stolen.
5. Defendant's negligence in failing to exercise reasonable care in protecting the PII of Plaintiff and the other Class Members is further evidenced by ***Defendant's failure to comply with legal obligations and industry standards***, and the delay between the date of the Data Breach and the time when the Data Breach was disclosed.
6. Furthermore, Defendant was negligent for waiting for more than five months to notify Plaintiff and similarly situated Class Members of the Data Breach.
7. Additionally, **Section 5 of the Federal Trade Commission Act ("FTCA") Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45, required Defendant to take reasonable measures** to protect Plaintiff's and the Class Member's PII data and is a further source of Defendant's duty to Plaintiff and

the Class Members. **Section 5 prohibits unfair practices in or affecting commerce, including, as interpreted and enforced by the FTC, the unfair act or practice by businesses like Defendant of failing to implement and use reasonable measures to protect Sensitive Information**. Defendant, therefore, was **required and obligated to take reasonable measures to protect PII** it solicited, possessed, held, or otherwise used. The FTC publications and data security breach orders described herein further form the basis of Defendant's duty to adequately protect Sensitive Information. By failing to implement and use reasonable data security measures, Defendant acted in violation of § 5 of the FTCA.

SECOND CAUSE OF ACTION *NEGLIGENCE PER SE*

1. Defendant's unreasonable data security measures and failure to timely notify Plaintiff and the Class of the Data Breach violates Section 5 of the FTC Act. Although the FTC Act does not create a private right of action, both require businesses to institute reasonable data security measures and breach notification procedures, which Defendant failed to do.
2. Section 5 of the FTCA, 15 U.S.C. §45, prohibits "unfair. . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by businesses like Defendant of failing to implement and use reasonable measures to protect users' sensitive data. The FTC publications and orders described above also form the basis of Defendant's duty.
3. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect users' personally identifying information and sensitive data and by not complying with applicable industry standards. Defendant's conduct was particularly unreasonable given the sensitive nature and amount of data it stored and the foreseeable consequences of a Data Breach should Defendant fail to secure its systems.

Common Law Causes of Action

- Breach of Fiduciary Duty
- Breach of Contract
- Breach of Implied Contract
- Negligence
- Negligence Per Se
- State Consumer Fraud Statutes

Regulatory Requirements

- FTC
- HIPAA
- DOL Guidelines
- State Cybersecurity Laws
- Privacy Laws

Regulatory Investigation

XXXX REPLY TO

DATA REQUEST

OCR Reference No. XXXX

1. If your organization has implemented "recognized security practices" that you wish OCR to consider as a mitigating factor in the resolution of a potential violation of the HIPAA Security Rule with an agreement, or in the determination of a proposed civil money penalty, please provide documentation demonstrating the implementation of such "recognized security practices." Also, please include an explanatory document identifying which submitted documents (or sections of documents) support the implementation of which specific elements (e.g., subcategories, sub-practices, controls) of the identified "recognized security practice." OCR suggests the following items to support your organization's position:

    a) Selection of which "recognized security practice" from below (i, ii, or iii) is being represented as implemented and documentation demonstrating implementation:

        i. Section 2(c)(15) of the National Institute of Standards and Technology Act;

        ii. The approaches promulgated under section 405(d) of the Cybersecurity Act of 2015;

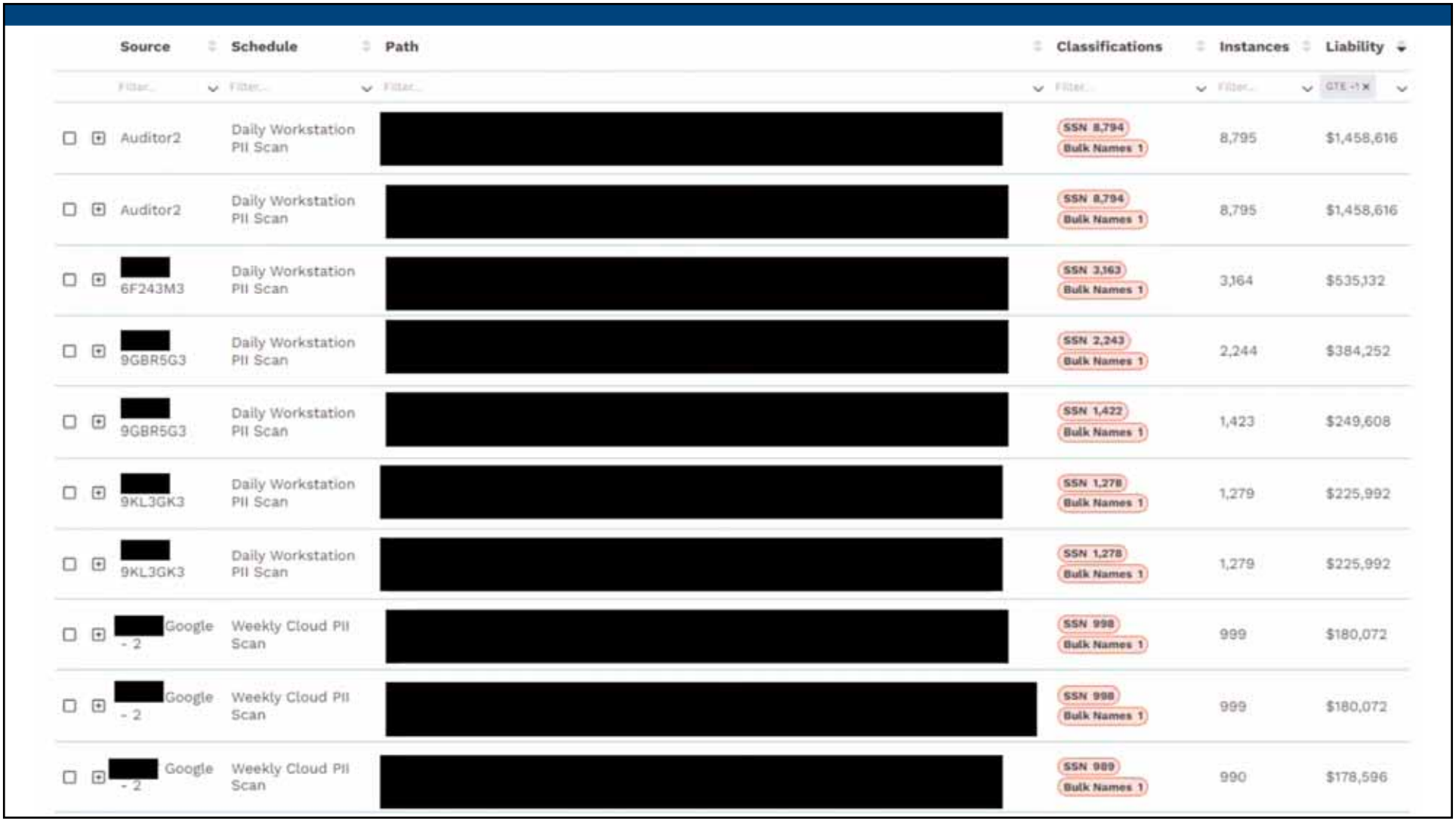
        iii. Other programs and processes that address cybersecurity that are developed, recognized, or promulgated through regulations under other statutory authorities. (Please provide regulatory or statutory citations.)

    b) Policies and procedures on implementation of "recognized security practices" including dates such policies and procedures went into effect.

    c) Project plans or similar documentation showing dates(s) of implementation (if specific elements of the entity's chosen "recognized security practices" are implemented on various dates, please provide specific dates for each element as applicable).

Result: $8.7 M Settlement

Potential Cost of a Breach

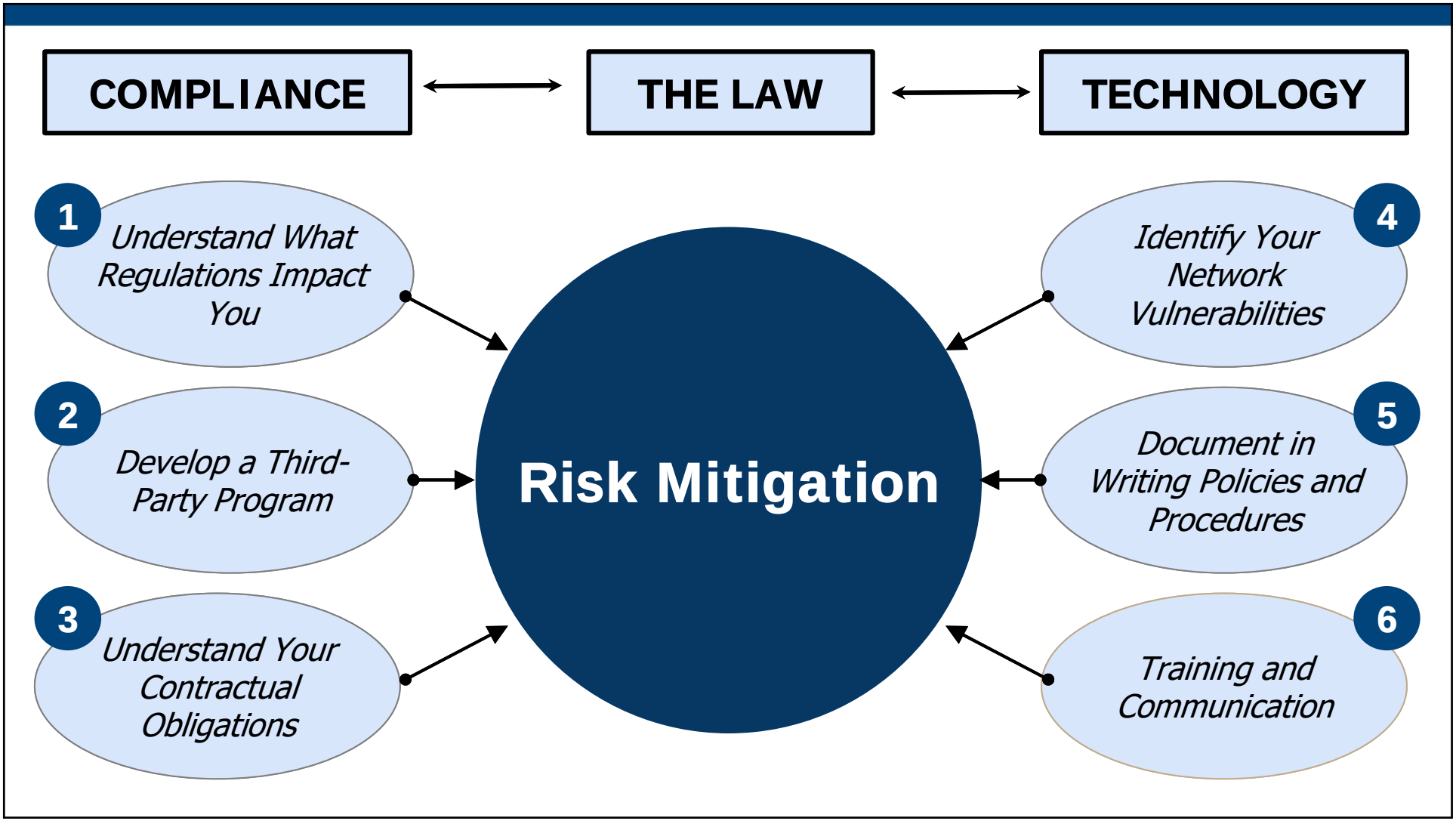


Source	Schedule	Path	Classifications	Instances	Liability
Auditor2	Daily Workstation PII Scan	[redacted]	SSN 8,794 Bulk Names 1	8,795	$1,458,616
Auditor2	Daily Workstation PII Scan	[redacted]	SSN 8,794 Bulk Names 1	8,795	$1,458,616
[redacted] 6F243M3	Daily Workstation PII Scan	[redacted]	SSN 3,163 Bulk Names 1	3,164	$535,132
[redacted] 9GBR5G3	Daily Workstation PII Scan	[redacted]	SSN 2,243 Bulk Names 1	2,244	$384,252
[redacted] 9GBR5G3	Daily Workstation PII Scan	[redacted]	SSN 1,422 Bulk Names 1	1,423	$249,608
[redacted] 9KL3GK3	Daily Workstation PII Scan	[redacted]	SSN 1,278 Bulk Names 1	1,279	$225,992
[redacted] 9KL3GK3	Daily Workstation PII Scan	[redacted]	SSN 1,278 Bulk Names 1	1,279	$225,992
[redacted] Google - 2	Weekly Cloud PII Scan	[redacted]	SSN 998 Bulk Names 1	999	$180,072
[redacted] Google - 2	Weekly Cloud PII Scan	[redacted]	SSN 998 Bulk Names 1	999	$180,072
[redacted] Google - 2	Weekly Cloud PII Scan	[redacted]	SSN 989 Bulk Names 1	990	$178,596

Why So Expensive?

- Forensic/Technical Investigation
- Legal
- Public Relations
- Notification
- Regulatory Fines/Penalties
- Regulatory Investigations
- Lawsuits

Practical Tips and Solutions


COMPLIANCE
THE LAW
TECHNOLOGY
1
Understand What Regulations Impact You
2
Develop a Third-Party Program
3
Understand Your Contractual Obligations
Risk Mitigation
4
Identify Your Network Vulnerabilities
5
Document in Writing Policies and Procedures
6
Training and Communication

Your Feedback Is Important.
Please Scan This QR Code.

Session Evaluation