

Cyber Risk and Commercial Banks: *An Evolving Exposure*

Presented by:

Justin Corey
Senior Vice President

 **NFP**
FINANCIAL INSTITUTIONS GROUP

August 24, 2023

BANKTALK 2023

BY THE SALTMARSH BANK ADVISORS

Saltmarsh
Saltmarsh, Cleaveland & Gund

 **NFP**



Financial Institutions Group – Current Locations and Client Distribution



by the numbers:



40+ employees | 7 offices



- 400+ equity protection clients;
- Credit Unions and Banks;
- \$3.4B+ in equity loans



600+ financial institution clients in all in 50 states



190+ loan portfolio lines clients



3 dedicated FI coverage attorneys



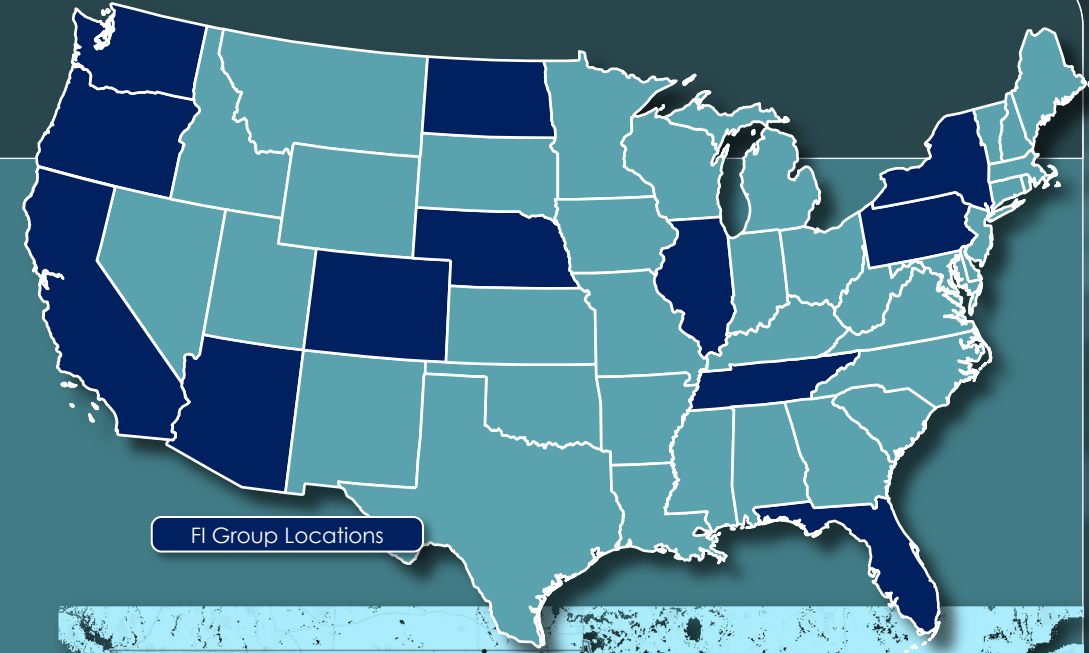
140+ commercial bank clients



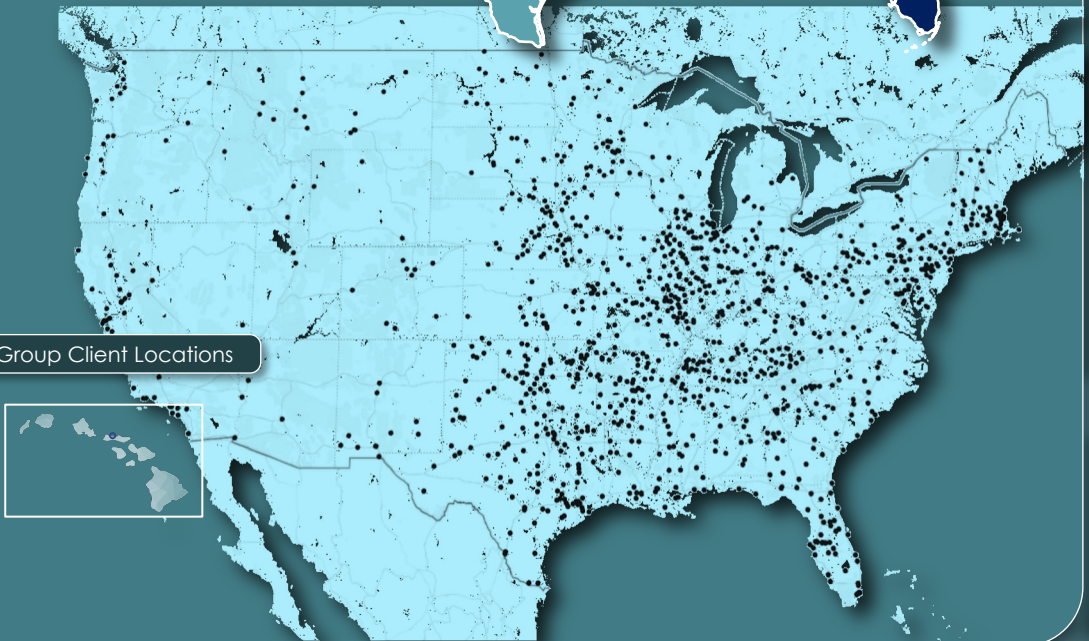
3 cyber risk specialists



50+ global carrier partners



FI Group Locations



FI Group Client Locations

SAMPLE POLICY STRUCTURE: Management Liability, Cyber Liability, FI Bond



So, what's the difference? When compared to most other industries, Banks have more policies and variables to consider when assessing their cyber insurance. Depending on the details of the claim, coverage could potentially be found within 3 different policies. Here are 3 claim examples to help illustrate the difference.

1 CLAIM SCENARIO

A bank employee inadvertently downloads a destructive computer virus onto the bank's network, resulting in widespread data loss. The bank catches the virus but not before 15,000 electronic records are compromised. After all costs incurred, the bank suffers a \$900,000 loss. **How did their insurance respond?**

2 CLAIM SCENARIO

A bank employee receives an email from a fraudster posing as an existing commercial customer requesting a wire transfer of \$1,750,000. The employee followed call-back procedures to verify the customer's identity. After confirming the call-back, the wire was sent to a bank in Manilla resulting in a \$1,750,000 loss. **How did their insurance respond?**

3 CLAIM SCENARIO

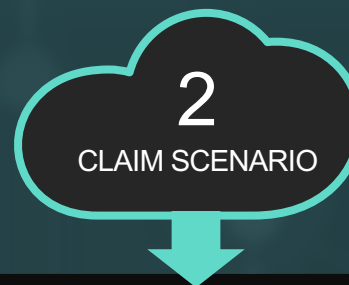
A bank officer inadvertently downloads an email attachment containing malware that compromises the bank's system. The fraudsters encrypt the bank's data and demand a ransom payment of \$1,000,000 in crypto currency to release the decryption key. **How did their insurance respond?**

OUTCOME: Each claim was covered under a different policy!

The bank needs to focus on their whole insurance program (not just the Cyber Liability policy) when addressing Cyber risk. Cyber Liability, Bankers Professional Liability and FI Bond policies are all critical components of a strong Cyber Insurance program. In fact, the majority of Computer Systems/Cyber claims are related to cyber crime and covered on the FI Bond (see slides 10 and 11).



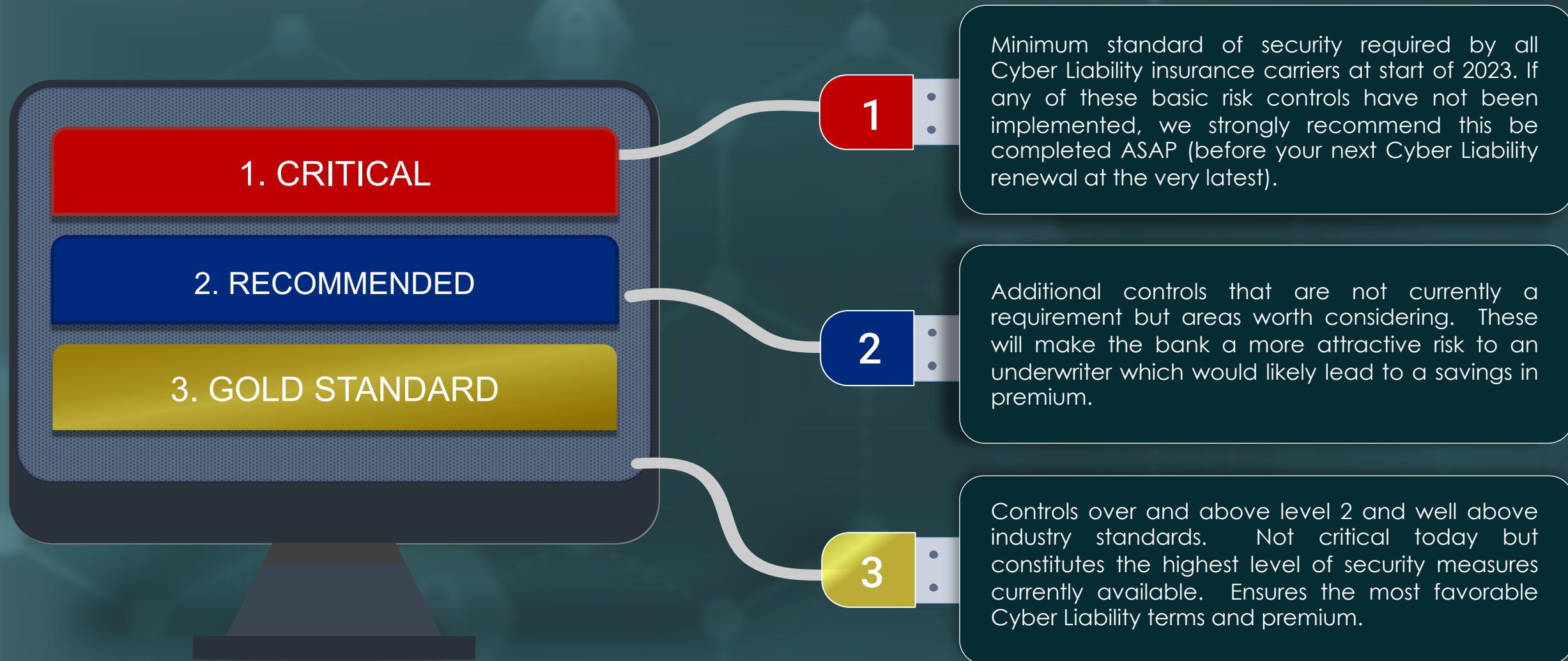
The Bank's **Cyber Liability policy** responds to cover the cost of the breach. This includes data forensics, notification expenses, cost of hiring a PR firm, legal fees, loss of income and a regulatory fine.

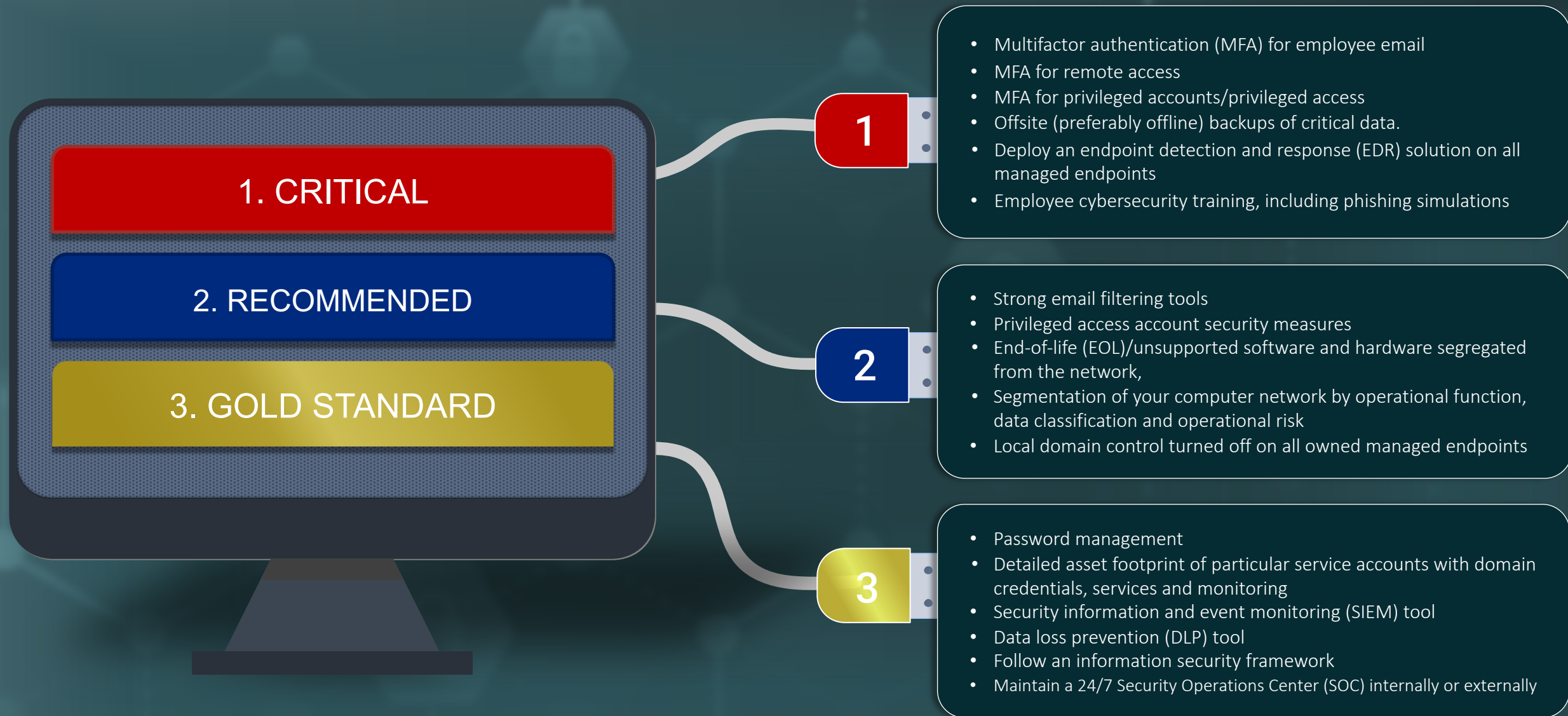


In this case, the bank's FI Bond did not respond as they did not include a social engineering endorsement as part of the bond. However, the customer sued the bank for negligence. **The Bankers Professional Liability policy did respond** to cover the bank's defense costs and a small award payment.



The bank carried \$2MM of Cyber Extortion coverage as part of their **Financial Institution Bond**. The \$2MM was sufficient to cover the ransom payment and any additional costs incurred as a result of the claim (PR Expenses, Notification Expense, Loss of Income, etc.)





BASELINE REQUIREMENTS OF CYBER LIABILITY INSURERS IN 2023

1. Secure remote network access via MFA for all remote access
 - a) Remote access to your network, applications, systems by employees, contractors and network service providers
 - b) Remote access to your data on cloud-hosted systems (i.e., software as a service, backups, etc.)
 - c) Remote access to your email, O365, Google, etc.
 - d) To access your VPN
 - e) On-premises access for privileged users
2. Backup and recovery assessment
 1. Air-gapped backups, taking into account cadence, segregation, testing and redundancy
3. Conducting regular employee infosec training, including quarterly phishing simulations
4. Endpoint protection (endpoint detection and response or EDR)
5. Incident response plans that include ransomware readiness (underwriters will want to know the plans have been tested as well)
6. Timely, consistent patch management protocols
7. Secure email configurations — DMARC, SPF, DKIM
8. Filtering inbound web traffic
9. Implementing least-privilege administrative models
10. Internal and external vulnerability scanning and secure remote desktop configurations
11. Segregating unsupported end-of-life software from primary network
12. Requiring callback verification for authorization of wire payments and any requested changes in routing information by third parties (call the previously known number on file, not a number provided via email request)

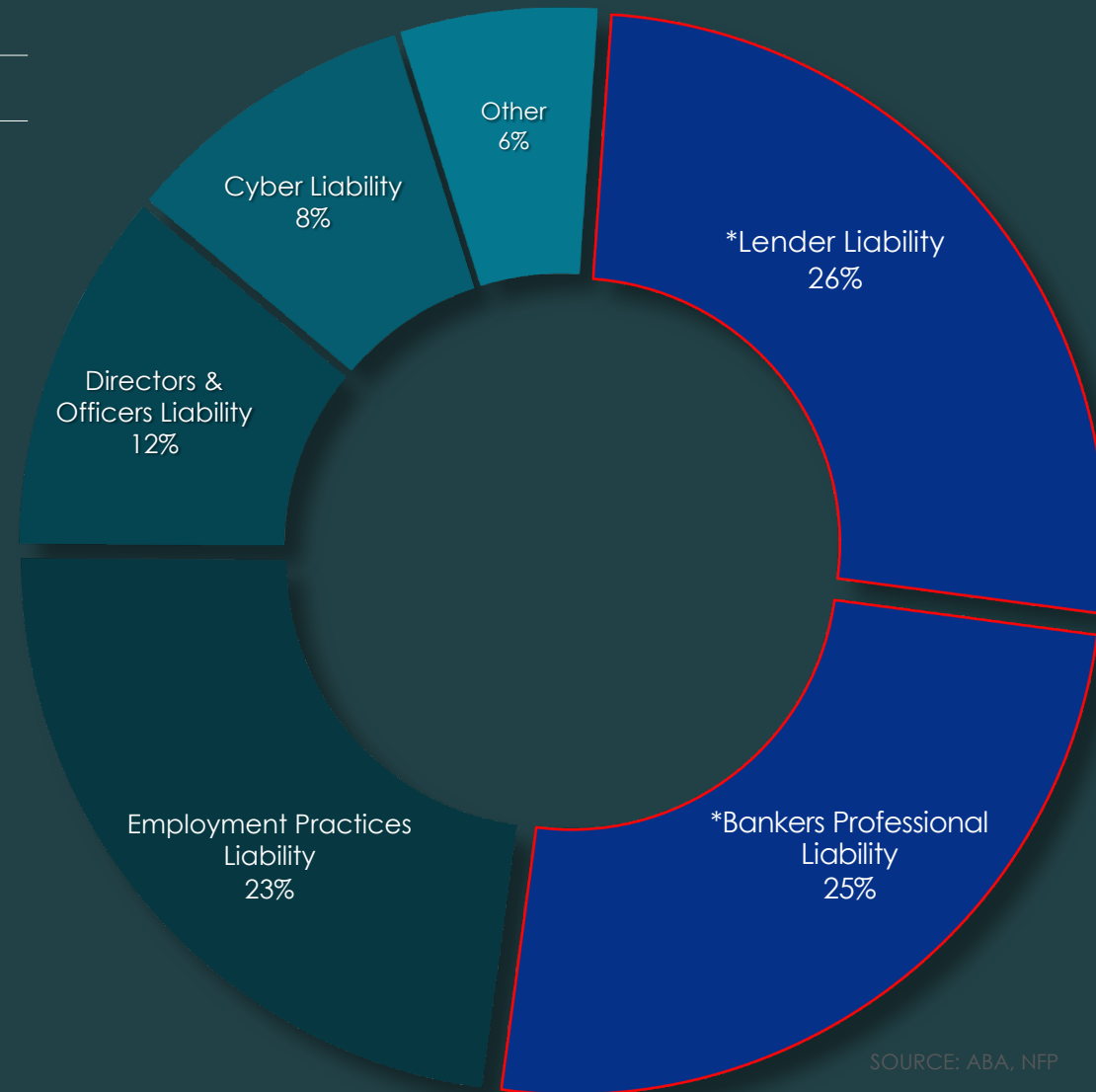
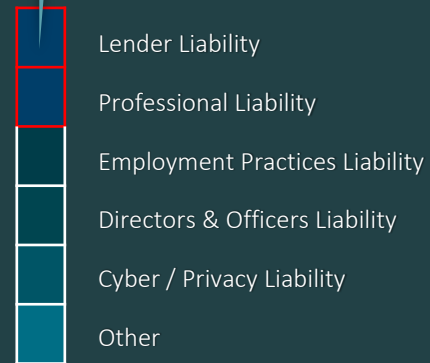
2022 Bank Claims Distribution: Management Liability

Management Liability Claims Distribution

Per Lines of Coverage

*SOURCE: ABA, NFP, TRAVELERS, INTACT, HALES REPORT

***Bankers Professional Liability**, which includes Lender Liability and Wire Transfer Liability, accounted for 51% of all Management Liability claims in 2022. Since BPL encompasses such a broad range of exposures, we ask that our bank clients review this coverage at each renewal to ensure they are comfortable with their limit.

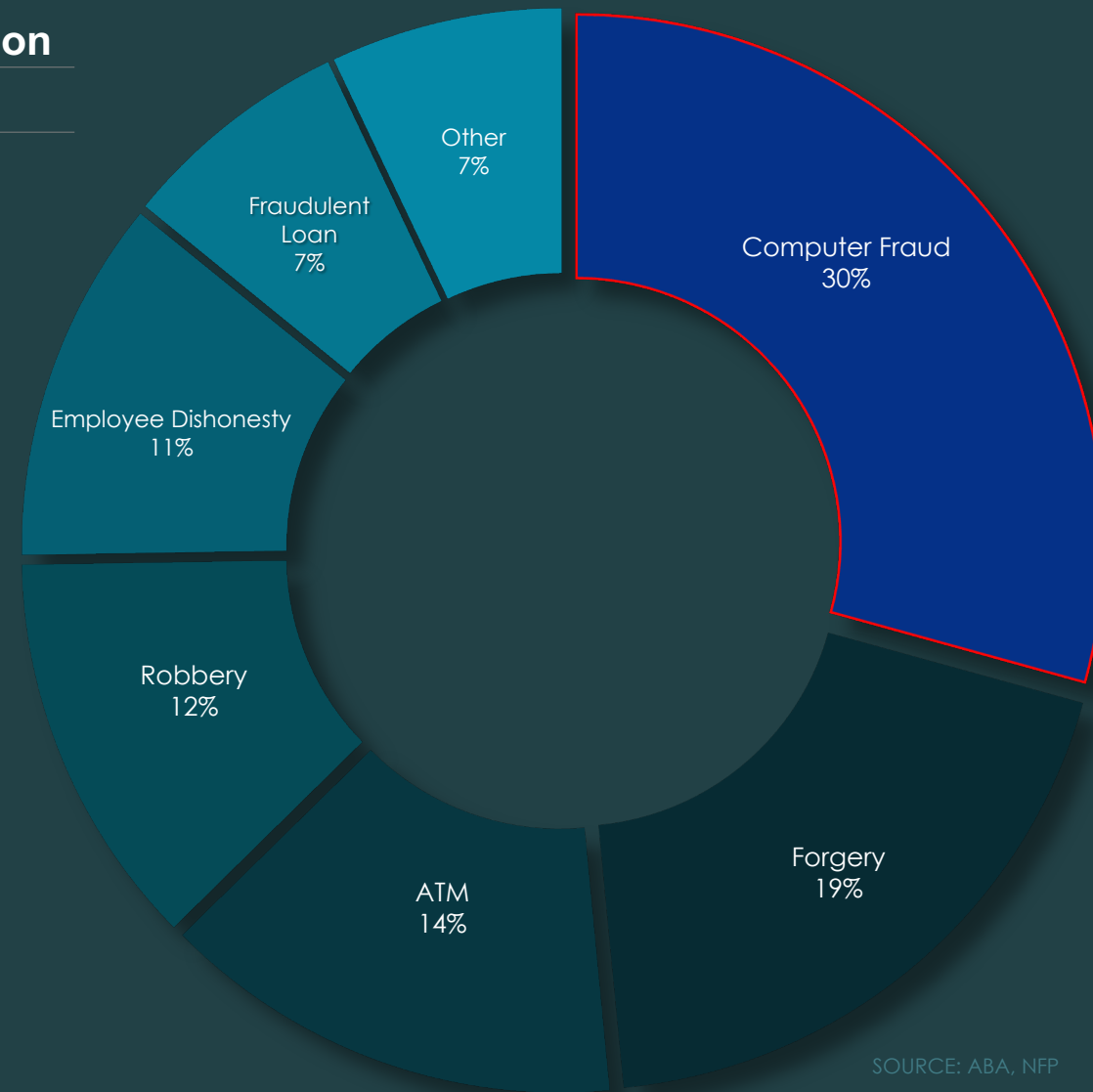
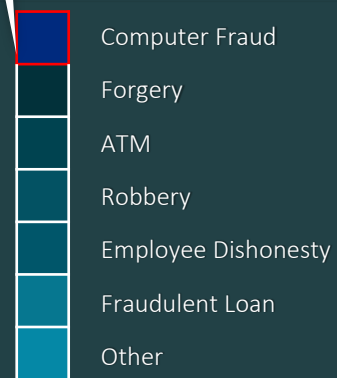


SOURCE: ABA, NFP

Financial Institution Bond Claims Distribution Per Lines of Coverage

*SOURCE: ABA, NFP, TRAVELERS, INTACT, HALES REPORT

***Computer Fraud** claims comprised 30% of all FI Bond claims filed in 2022. Common Computer Fraud losses may include Wire Transfer Fraud, Voice (or Email) Initiated Transfer Fraud, Unauthorized Mobile Banking Fraud, and/or Destruction of Program/Data by a Hacker or Virus.



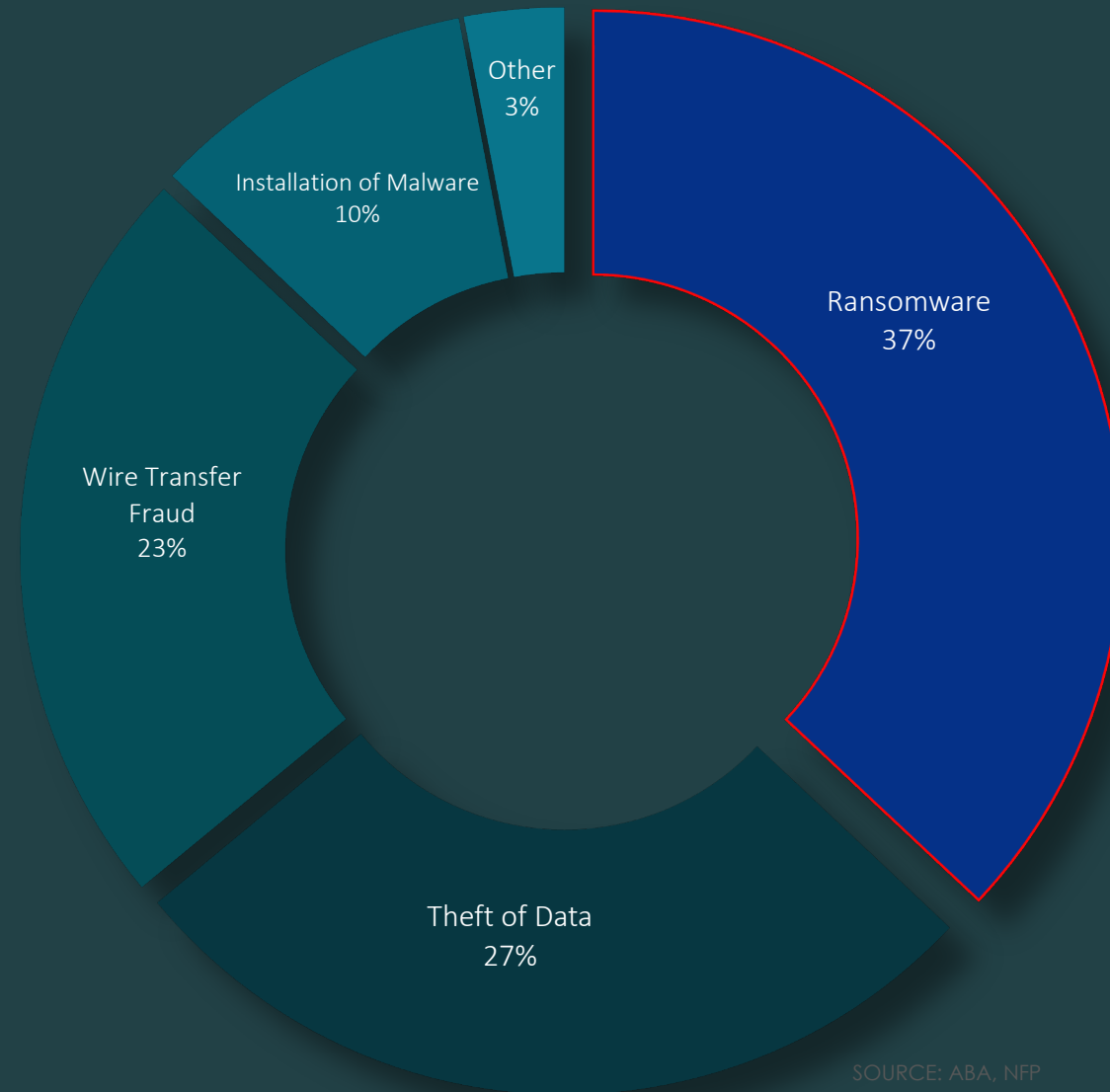
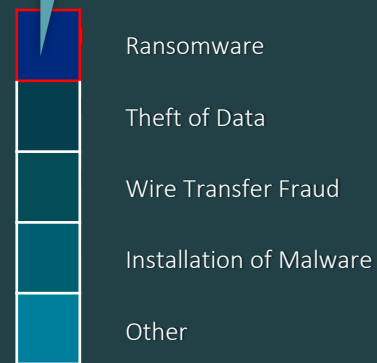
SOURCE: ABA, NFP

FI Cyber Liability Incident Response

Per Lines of Coverage

*SOURCE: ABA, NFP, TRAVELERS, INTACT, HALES REPORT

Ransomware now represents 37% of all Cyber Liability claims handled, compared to 27% in 2021. Banks should accelerate their efforts to put effective mitigation measures in place. These include multi-factor authentication (MFA), endpoint detection and response tools, patch management protocols, and robust backup plans.



SOURCE: ABA, NFP

Insuring Agreements Explained

Insuring Agreement	Security & Privacy Liability	Privacy Regulatory Defense, Awards and Fines	Media Content	Event Management	Cyber Extortion	Network Interruption
What is Covered?	Defense costs and damages arising out of a data security or privacy incident to a third party, including fines and/or penalties arising out of PCI-DSS non-compliance.	Coverage for claim expenses and regulatory damages as a result of a privacy regulatory action (violations of GDPR, CCPA, and/or BIPA).	Defense costs and damages for third party claims alleging libel, slander, copyright/trademark infringement, invasion of privacy, etc. arising out of all content distributed by a company.	Costs incurred arising from a cyber incident, including costs to hire expert privacy counsel to determine any legal obligations, costs to retain a forensic firm to investigate the cause of the event, notification and call center costs as well as public relations.	Money paid by you, including cryptocurrency with the insurer's consent to resolve a cyber security threat and costs to investigate the cause of the threat.	Loss of income and extra expenses incurred by you following a security or system failure of your computer systems, subject to a waiting period and/or monetary retention.
Types of Claims	Privacy Class Actions: <ul style="list-style-type: none"> • Neiman Marcus • Anthem PCI-DSS Related Litigation / Demands <ul style="list-style-type: none"> • Target • Home Depot 	Regulatory Actions including: <ul style="list-style-type: none"> • State Attorneys Office of Civil Rights under HIPAA • EU Countries under GDPR 	Most common examples include demands to cease and desist using imagery and/or claims for copyright or trademark infringement.	Most common examples include hiring a forensic investigation specialist to conduct an investigation at an hourly rate. Setup and implementation costs of notifying individual consumers, including setting up new call centers to handle volume.	Most common examples include extortion demands following a ransomware attack.	Merck and Maersk impacted by NotPetya ransomware Nation-state attacks against Sony Pictures Entertainment Royal Bank of Scotland 2012 outage Azure or AWS or other data center outage impacts your operations

FI Pricing Trends by Core Coverage Line (3Q18 – 1Q23)

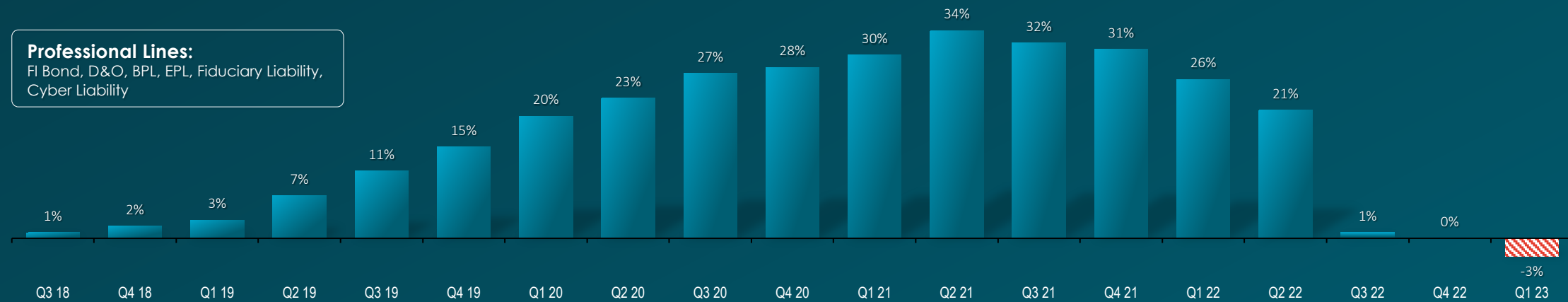
Financial Lines Pricing Trends

Per Lines of Coverage

*SOURCE: ABA, NFP, TRAVELERS, INTACT, HALES REPORT

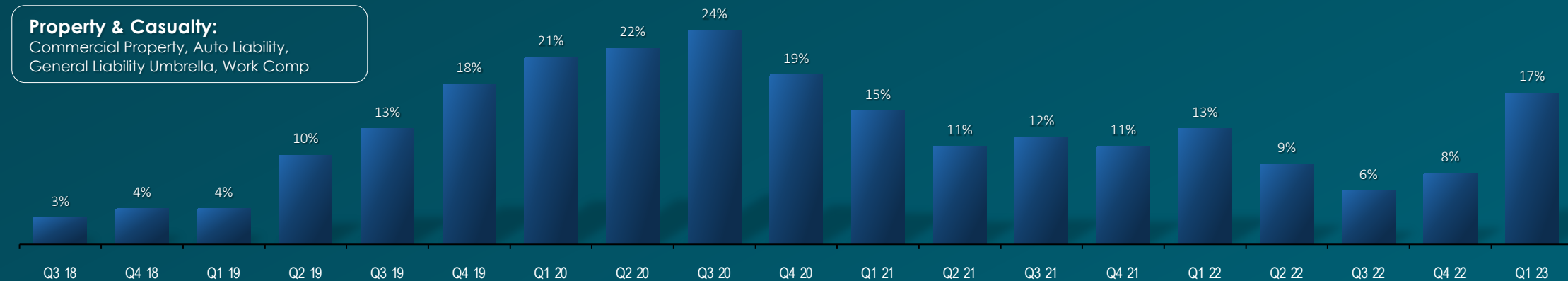
Professional Lines:

FI Bond, D&O, BPL, EPL, Fiduciary Liability, Cyber Liability

















Property & Casualty:

Commercial Property, Auto Liability, General Liability Umbrella, Work Comp



NFP FI GROUP - STANDARD CARRIER LIST 2022

NFP's Financial Institutions Group only contracts with financially strong insurance carriers with a minimum AM Best® Financial Strength Rating of A- (Excellent) and Financial Size Category XII (\$1 Billion in policy holder's surplus). All of our standard carriers use community bank-specific insurance forms and have dedicated Financial Institution underwriting divisions. We also have appointments with global surplus lines carriers that provide specialized coverages, i.e. Cyber Liability, Debit Card Fraud and Kidnap & Ransom. These carriers are held to the same financial strength and claims-paying criteria as our standard, admitted carriers. Having the industry's broadest market access is critical for negotiation purposes and continually evolving carrier appetites. Please see page 26 for a complete list of NFP's FI Group global insurance carrier partners.

CARRIER	 Financial Strength	 Financial Size Category
 Great American	A+ (Superior)	FSC XV (\$2 Billion+)
 CNA	A (Excellent)	FSC XV (\$2 Billion+)
 Travelers	A++ (Superior)	FSC XV (\$2 Billion+)
 Intact/OneBeacon	A+ (Superior)	FSC XV (\$2 Billion+)
 Berkley	A++ (Superior)	FSC XV (\$2 Billion+)
 Markel	A (Excellent)	FSC XV (\$2 Billion+)
 Chubb	A++ (Superior)	FSC XV (\$2 Billion+)
 Zurich	A+ (Superior)	FSC XV (\$2 Billion+)
 Hanover	A (Excellent)	FSC XV (\$2 Billion+)
 AmTrust	A- (Excellent)	FSC XV (\$2 Billion+)
 Everest	A+ (Superior)	FSC XV (\$2 Billion+)
 AIG	A (Excellent)	FSC XV (\$2 Billion+)

DIRECTORS & OFFICERS LIABILITY (D&O)

Directors and officers (D&O) liability insurance protects the personal assets of corporate directors and officers, and their spouses, in the event they are personally sued by employees, vendors, competitors, investors, customers, or other parties, for actual or alleged wrongful acts in managing a company.

D&O insurance covers legal fees, settlements, and other costs. D&O is the financial backing for a standard indemnification provision, which holds officers harmless for losses due to their role at the bank.

Directors and officers are sued for a variety of reasons related to their company roles, including

- Breach of fiduciary duty resulting in financial losses or bankruptcy
- Misrepresentation of bank assets
- Misuse of bank funds
- Fraud
- Failure to comply with workplace laws
- Theft of intellectual property and poaching of competitor's customers
- Lack of corporate governance

Illegal acts or illegal profits are not covered under D&O insurance

Side-A: Directors and Officers Liability

Side-A, also known as "Individual" D&O, is the first insuring agreement of a D&O policy. Side-A protects executives from claims when corporate indemnification is not available from their organization. As non-indemnification can occur for many reasons, Side-A coverage plays an important role in protecting individuals when this financial support is not available.

Side-B: Corporate Reimbursement

Side-B, also known as corporate reimbursement, is the second insuring agreement of a D&O policy. Side-B reimburses an organization for the expenses it occurs when defending its management in accordance with its corporate indemnification obligations. By indemnifying its executives, an organization is responsible for paying all legal expenses and claim settlements on their behalf. The costs of doing this can be impairing for even the largest of organizations and can potentially affect its financial stability. Side-B coverage, therefore, supports an organization financially when it is, in turn, supporting its management.

Side-C: Entity Securities coverage

Some D&O policies also include a third insuring agreement, Side-C, also known as entity securities coverage. Side-C coverage is typically reserved for publicly listed companies and protects the corporate entity from its own liability exposures.

The coverage provided by Side-C is limited to claims made against a company as a result of the offer, sale or purchase of its securities; in other words, the shares listed on the stock market available for purchase by investors.

CLAIM EXAMPLE: Two brothers entered into an agreement to purchase a property and develop it into an antiques mall. The brothers met with a director of the local bank to express their desire to obtain a loan to assist in their endeavor. Unbeknownst to the brothers, the property was subject to a right of first refusal by a nonprofit entity which ultimately purchased the property. The brothers discovered the bank director's wife sat on the board of the nonprofit organization and, subsequently, filed a lawsuit against the bank director. They alleged the director breached a duty of good faith and fair dealing and otherwise engaged in fraud and conspiracy to violate their civil rights. The director was covered by the bank's D&O policy. Though the Court ultimately dismissed all claims against the director, his defense racked up \$220,000 in legal fees.

Source: ABA Insurance Services

BANKERS PROFESSIONAL LIABILITY (BPL)

Bankers Professional Liability (BPL) is a type of errors and omissions coverage written for banks and financial institutions. The policies cover economic losses resulting from mistakes committed in providing financial services that include, but are not limited to, acting as a wire transfer or escrow agent; consumer financial, tax, or estate planner; trustee under a bond indenture; and providing electronic data processing services. Although the term "bankers professional liability" insurance (BPL) is often used interchangeably with "trust department errors and omissions liability insurance," the latter is actually a subset of BPLI. This is because coverage for liability arising from a bank's trust department is only one of the many kinds of insurance provided under BPL forms.

Claim Example: A commercial customer filed a complaint against a bank alleging that the customer's former controller embezzled over \$300,000 by making withdrawals from a deposit account it held at the bank. The Complaint alleged that the withdrawals were highly suspicious in nature but the bank never contacted other officers of the firm to inquire whether the transactions were appropriate. Further, the Complaint alleged that the fraud could not have occurred without the knowledge and involvement of the bank. The customer sought compensatory and other damages. The Complaint was ultimately dismissed in court, but not before the bank incurred \$60,000 in defense costs. materials.

LENDER LIABILITY

Often contained within Bankers Professional Liability (BPL), Lender Liability provides the coverage for errors and omissions arising out of the extension of credit. Since lending activity is excluded from the BPL policy, Lender Liability needs to be included as a separate, distinct coverage. BPL and Lender Liability often share a single limit so we recommend the bank pay particular close attention to ensure they are comfortable with the amount of coverage provided.

Claim Example: A customer claimed that a bank refused to make advances on an \$8 million construction loan after making one initial advance for the stated reason that the interest rates negotiated by its loan officer were too low. In his Complaint, the customer made claims of breach of contract, material misrepresentation, and violations of the consumer fraud laws against both the bank and the loan officer. He demanded compensatory damages and other damages, attorneys' fees and costs, interest and reimbursement of professional fees. The customer refused the bank's initial attempts at restructuring the loan but through mediation, all parties ultimately agreed to mutually acceptable loan terms. \$281,000 was paid by insurance to defend and settle the matter.

EMPLOYMENT PRACTICES LIABILITY

Covers wrongful acts arising from the employment process. The most frequent types of EPL claims reported include: wrongful termination, discrimination, sexual harassment, and retaliation.

Claim Example: A former internal auditor of a bank filed suit in a U.S. District Court alleging retaliation in violation of Sarbanes-Oxley. The auditor contended that her supervisor substantially revised her year-end SOX reports, effectively removing the compliance issues she had identified. She alleges that she reported her supervisor's actions to HR. She further alleges that after years of positive performance evaluations, the bank terminated her employment in retaliation of her whistleblowing activities. The case went to court and plaintiff was paid \$110,000 for loss of income and emotional distress and \$510,000 for reimbursement of attorney's fees and expenses.

FIDUCIARY LIABILITY

Under the Employee Retirement Income Security Act of 1974 (ERISA), fiduciaries can be held personally liable for losses incurred in an employee benefit plan where such losses were incurred as a result of the fiduciaries' alleged errors, omissions or breach of fiduciary duties. Fiduciary Liability insurance provides coverage for judgments, settlements and defense costs arising from the administration of these plans or the violation of any responsibilities or duties imposed by ERISA and similar laws.

Claim Example: A bank employee sues his employer for negligence and attempts to recover lost health-care benefits because the bank failed to enroll him in its medical plan. The amount of \$14,000 was paid to settle the matter.

TRUST SERVICES LIABILITY

Trust Services Liability is also typically included under the Bankers Professional Liability, covers wrongful acts arising out of errors and omissions of the bank's Trust Department. Examples of acts that may give rise to such liability include improper investment of trust assets, failure of a stock transfer agent to effect the transfer in the required time limit, and permitting devaluation of trust assets.

Claim Example: A bank was advised by its accountant to convert to S-Corp status and the bank commenced the process of conversion. At the time of conversion, some shareholders held their bank shares in an IRA. Unfortunately, the conversion had negative tax consequences for the shareholders about which they were never advised. For most of these "IRA shareholders", the bank's Trust Department is the custodian and financial advisor. The shareholders made demands for damages. The bank settled the claims made by the impacted individuals. Insurance provided defense and settlement coverage up to the policy limits of \$1,000,000. Later, the bank and the insurance company pursued a subrogation recovery against the accountant, and made a significant recovery.

FINANCIAL INSTITUTION BOND (CRIME)

FIDELITY COVERAGE (EMPLOYEE DISHONESTY)

Covers dishonest or fraudulent acts committed by employees. Employee dishonesty claims consistently rank as the most frequently reported type of Bond Claim, even in this age of rampant cyber fraud. It remains the most important part of a bank's Bond coverage.

Claim Example: Over the course of 6 months, a branch manager stole \$112,000 from the bank's vault by smuggling stacks of \$100 bills out and throwing them in the trash. The manager would subsequently retrieve the stacks and replace the inner \$100 bills with \$1 bills, leaving the top and bottom \$100 bills. She then placed the tampered and devalued stacks back into the vault. The fraud was ultimately discovered by the back-up branch manager while selling money to a teller.

ON PREMISES - THEFT & DISAPPEARANCE

Covers losses resulting from burglary, robbery, theft, misplacement or mysterious disappearance of property located on bank premises.

Claim Example: A takeover-style armed robbery resulted in the loss of \$187,000 in vault cash.

IN TRANSIT - THEFT & DISAPPEARANCE

Covers losses of certain property while in transit if a result of robbery, theft, misplacement, mysterious disappearance, or destruction.

Claim Example: A bank employee is robbed of funds when delivering cash and coin from the main office to a branch office.

COUNTERFEIT MONEY

Covers losses resulting from the bank having received, in good faith, counterfeit currency.

Claim Example: A customer deposits \$8,000 of counterfeit cash in an ATM over the course of several weeks. Subsequently, the customer withdraws the cash in \$2,000 increments from 4 other ATMs in 4 other locations. The bank ultimately sells the \$2,000 to the Fed to lighten some of its cash reserves. The Fed rejects the cash as counterfeit. The bank has now suffered a \$8,000 loss.

UNAUTHORIZED SIGNATURES

Covers losses resulting from the bank honoring negotiable instruments or withdrawal orders that bear signatures of unauthorized individuals (individuals whose signatures are not reflected on the appropriate signature card).

Claim Example: A bookkeeper of a corporate customer signs her name as maker on a company check and deposits the funds into her personal account. When the bookkeeper disappears with the funds, the bank is held liable for the funds, as the bookkeeper is not an authorized signatory on the account. (Note that the loss would not be covered under Insuring Agreement D's forgery coverage as no forgery was committed.)

FORGERY OR ALTERATION

Covers losses resulting from forgery or alteration of negotiable instruments.

Claim Example: A bookkeeper of a corporate customer signs the business owner's name on a company check and deposits the funds into her personal account at another bank. The forgery is detected when the business owner reviews his monthly statements.

CYBER LIABILITY / ELECTRONIC PRIVACY LIABILITY

CYBER LIABILITY

Provides cover for demands related to system security issues that aren't privacy related, such as denial of service attacks and virus transmissions.

Claim Example: business customer's computer systems contracted a virus from accessing the bank's on-line banking platform.

DATA BREACH LIABILITY

Provides cover for lawsuits and related demands stemming from the unauthorized access of confidential information. The unauthorized access may come from a breach of the bank's systems, a breach of a service provider's system, or other errors or omissions on the party of the bank.

Claim Example: The bank's internet banking provider experiences a hack resulting in the unauthorized exposure of personal information of the bank's on-line platform customers. The customers sue the bank for failure to provide adequate security measures.

ELECTRONIC FUNDS TRANSFER LIABILITY

Provides cover for demands related to wrongful acts committed in connection with the transfer of customer funds.

Claim Example: Funds from a customer deposit account are wired to a third party bank based upon fraudulent authorization utilizing the stolen credentials of an authorized employee. The customer demands restitution for his \$40,000 loss.

CYBER PUBLISHING AND SOCIAL NETWORKING LIABILITY

Provides cover lawsuits related to information electronically displayed or disseminated through the bank's website or social networking accounts.

Claim Example: The bank's internet banking provider experiences a hack resulting in the unauthorized exposure of personal information of the bank's on-line platform customers. The customers sue the bank for failure to provide adequate security measures.

REGULATORY DEFENSE

Provides coverage for defense costs for a demand brought by certain regulatory agencies in connection with data breaches or the compromise of confidential customer information.

Claim Example: In the wake of a system breach resulting in the exposure of confidential customer information, the bank's regulators allege that the bank had inadequate security controls. In addition, the FTC alleges the bank committed several violations of laws designed to protect the privacy of customer information. The costs to defend the FTC's complaint totaled \$75,000.

PRIVACY AND SECURITY BREACH RESPONSE EXPENSES

Provides expense reimbursement to the bank for certain costs incurred to identify, stop and remedy a system breach.

Claim Example: 23,000 private financial customer records were stolen from the bank's systems by an international cyber-criminal group. The bank incurred costs of \$140,000 to retain a remediation team, including privacy attorneys and forensic investigators, and an additional \$66,000 to notify impacted customers and provide credit protection services.

CYBER LIABILITY / ELECTRONIC PRIVACY LIABILITY

BUSINESS INTERRUPTION

Coverage indemnifies the bank for lost income and extra expenses arising from system interruptions caused by hackers.

Claim Example: A computer virus shuts down the bank's on-line banking platform. The website is down for 72 hours as programmers rewrite, test, and elevate new code. In the interim, the bank extends branch hours to accommodate those who normally bank on-line in the evenings. Insurance covered the bank for the net proceeds that would have been earned, absent the system disruption, after the first 24 hours system of downtime. Insurance proceeds also covered the extra expenses incurred to conduct business during the system outage.

CYBER EXTORTION

Coverage indemnifies the loss of property surrendered as a result of cyber threats.

Claims Example: A bank decides to not extend credit to a business customer. In retaliation, the custom announces it has access to the bank's systems and threatens to publish confidential customer information unless the bank transfers \$250,000 to its Cayman Island accounts. The claim is covered by Cyber Extortion.



THANK YOU

 **NFP**[®]
NFP.com