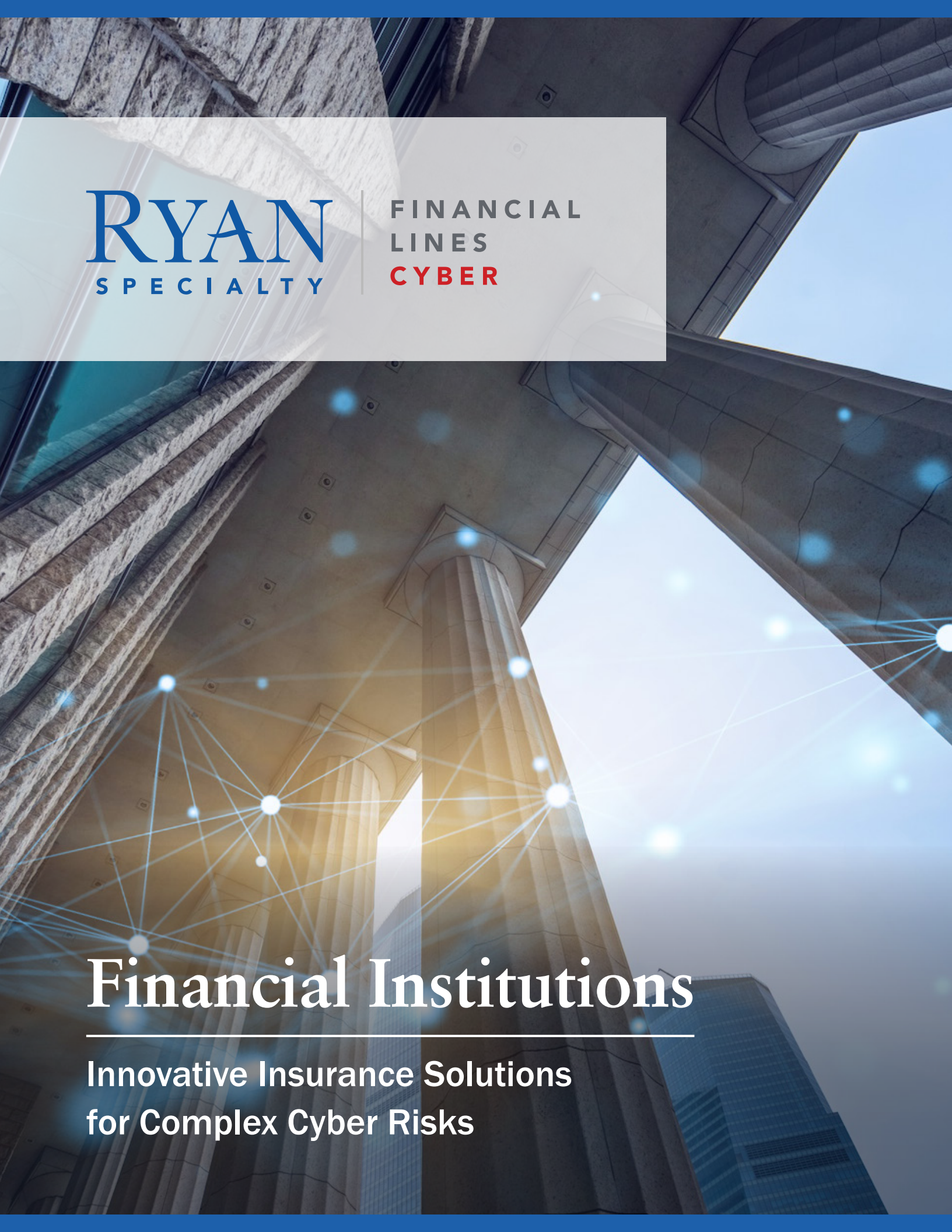

RYAN SPECIALTY

FINANCIAL LINES CYBER

Financial Institutions

Innovative Insurance Solutions for Complex Cyber Risks

RYAN SPECIALTY | FINANCIAL LINES CYBER

Cyber Exposure for Financial Institutions

More than just money is at stake.

Financial institutions don't just guard capital — they safeguard vast troves of sensitive data. From customer records in retail banks to proprietary strategies in investment firms, the sector is a prime target for sophisticated cyber attacks.Mega-banks operate around the clock, across continents, processing trillions of data points daily. Yet, many still rely on fragmented IT systems, underfunded security infrastructure, and patchwork integrations, which can leave critical vulnerabilities exposed. Efficiency-driven models often prioritize accessibility over control, making traditional perimeter-based security models obsolete.

Key challenges include:

- Diverse risk profiles across retail, investment, and digital banking
- Third-party exposure from fintech partnerships and vendor ecosystems
- AI-powered phishing campaigns that outsmart legacy defenses
- Budget constraints that limit proactive investment in cybersecurity

The result is a complex, high-stakes environment where a single cyber breach can trigger regulatory penalties, reputational damage, and massive financial loss. Modern financial institutions need modern cyber strategies that are resilient, adaptive, and built for a borderless digital world.

Cyber risk isn't one-size-fits-all in banking.

Different types of banks face different cyber challenges. A retail bank's operations, revenue streams, and customer interactions differ significantly from those of an investment bank, and so do their data environments and risk profiles. As a result, the financial and operational fallout of a cyber breach can vary dramatically across institutions. Adding to the complexity, banks increasingly rely on fintech partnerships and third-party vendors, which can introduce hidden vulnerabilities. Without rigorous vetting, like penetration testing, these external connections can become weak links in an otherwise secure system.

Meanwhile, AI-powered phishing attacks are raising the stakes. Cybercriminals now use advanced tools to craft highly convincing messages, making it easier than ever to trick employees into sharing sensitive information. In today's evolving threat landscape, banks are wise to tailor their cybersecurity strategies to their business models, data flows, and digital ecosystems to avoid potentially being outpaced by attackers.

Retail Banks focus on consumers as customers.

- Store large amounts of personally identifiable information (PII), account and credit card information
- Must operate 24/7 for customers access to their funds
- Maintain large customer web-based platforms to allow clients to manage their accounts and apply for financial products
- Employ call centres with the ability to access account information to support clients
- Experience high turnover at the service level, such as tellers
- Are heavily regulated to ensure consumer confidence

Commercial Banks focus on business customers.

- Serve larger, complex customers than those served by retail banks, often making them a target of interest for cybercriminals
- Accept payments from customers and rely heavily on lines of credit to manage cash flow
- Tend to hold less PII, however might hold proprietary information around customers' business activities
- Earn revenue from non-interest income, such as financing lines of credit

Investment Banks help businesses work in financial markets.

- Represent the interests of many different types of investors from commercial institutions to state owned entities to high-net-worth individuals
- Store large amounts of proprietary information on behalf of their clients, which can make them targets for state-sponsored actors
- Require instant access to capital markets and trading platforms to help clients create markets
- Can earn fees which contributes to a percentage of earnings

Credit Unions are not-for-profit organizations owned by their customers.

- Offer products and services similar to most retail and commercial banks
- Online Banks operate entirely online
- Offer competitive rates on savings accounts
- Often offer free checking to customers
- Share exposures with retail banks

Online Banks operate entirely online.

- Offer competitive rates on savings accounts
- Often offer free checking to customers
- Share exposures with retail banks

Illustrative Claims Scenarios

PRIVACY BREACH

Outdated Systems, Costly Breach

A credit union failed to update its systems for over two years. A hacker exploited a known vulnerability, gaining access to sensitive customer data, including financial records and personally identifiable information. This resulted in a breach with serious consequences.

PHISHING

Deceptive Email, Detrimental Breach

An employee at a local bank received an email appearing to be from a regional manager, requesting a compliance-related download. Without verifying the sender, the employee opened the attachment, unleashing malware that silently exfiltrates sensitive customer financial data. One click compromised an entire network.

PRIVACY BREACH

One open port. One third-party vendor. One significant breach.

When a bank handed over full network access to a vendor, a hacker found the weak link, slipped through an exposed port, and obtained sensitive customer data.

These examples are hypothetical scenarios used solely to illustrate potential outcomes and not reflective of policy terms and conditions or the facts of a specific claim.

RFL's Cyber Solution

Cyber risk is no longer hypothetical. It's operational. Ryan Financial Lines' (RFL) cyber insurance policy treats cyber as a core peril, not an afterthought. Designed with the banking sector in mind, our coverage is tailored to help address a full spectrum of digital threats, including business interruptions, data restoration, computer crime, social engineering, extortion, and privacy breaches. What sets us apart? A best-in-class blend of first-party cost reimbursement and third-party defense and regulatory coverage, powered by broad definitions of data and computer systems.

1ST PARTY

Crisis Response: Intended to help mitigate the costs and expenses to respond to a system event or privacy breach event

Cyber Extortion: Intended to help mitigate the costs and expenses to respond and resolve an extortion demand that threatens to release or destroy data and / or disrupt or damage the computer system

Computer System Interruption: Intended to help mitigate the net income losses and additional operating costs that occur during a business interruption event due to systems and/or data being taken offline in a malicious attack or other operational failure. Coverage may include:

- Renting, leasing or hiring external equipment to reduce the duration of a material interruption
- Additional operating costs including services, premises, employing contract staff, and overtime cost
- Costs to switch service from a named IT vendor to a new provider if the service cannot be restored within the indemnity period (when event is caused by vendor systems)
- Procuring product or services from alternative sources to meet contractual obligations in supplying the insured's customers
- Paying any service credits or contractual penalties that the insured is contractually required to pay as a result of a material interruption

Reputational Damage: Intended to help mitigate the direct loss of net income due to a reduction in business or the loss of a service contract with a client in the wake of the public being notified of a system event, privacy breach event, or network security event

Fraud and Social Engineering: Intended to help mitigate the direct financial loss from the wrongful transfer of money by fraudulently accessing the computer system or intentionally misleading an authorized person to transfer funds to a third party purporting to be a vendor, client, or employee. This cover also extends to the financial loss arising from the unauthorized access of a client's telecommunication system by a malicious third party

Data and Software Restoration: Intended to help mitigate the costs and expenses to recover corrupt data or software, and potentially even upgrading / replacing affected software applications or equipment

3RD PARTY

Privacy Breach and Other Third-Party Liability: Intended to help mitigate the defence costs and damages arising from:

- Any unauthorized disclosure or access to personal or confidential corporate data
- Any liability that arises from other cyber events such as the transmission of a malicious code, contract breaches due to a business interruption (BI) event, and unauthorized access to data by a third party

Vendors

In a cyber crisis, speed and precision matter, and RFL's cyber solution is built to help provide banks with seamless access to best-in-class vendors and a frictionless claims experience. We don't stop at response. We aim to help you stay ahead of the threat. Our thorough breach response coverage is paired with a curated panel of expert resources who work proactively to reduce your exposure and to help minimize the impact if an incident occurs.

Privacy Counsel: US

Pierson Ferdinand LLP

Incident reporting:

RFLCyber@pierfed.com

833-737-7444

Alternate counsel options:

McDonald Hopkins LLC

Cipriani & Werner, PC

Mullen Coughlin

Wood Smith Henning & Berman LLP

Privacy Counsel: Intl.

Kennedys Law LLP

Incident reporting:

RyanFinLinesIR@kennedyslaw.com

UK/EMEA- +44 203 137 8749

AUS/APAC- +613 9498 6688

Alternate counsel options:

Weightmans LLP

Pinsent Masons LLP

Forensics: US

CyXcel

S-RM

Kroll

IronGate

CrowdStrike

PNG Cyber

Palo Alto Networks - Unit 42

Data Mining

CyXcel

Consilio

Asceris

Epiq

Notifications

IDX

Epiq

Kroll

Forensics: Intl.

CyXcel

S-RM

Please note that the use of these vendors is subject to the terms, conditions, and reporting requirements outlined in your policy. We reserve the right to amend our vendor panel at any time.

RYAN SPECIALTY | FINANCIAL LINES CYBER

Who We Are

Ryan Financial Lines (RFL) was formed in March 2024 to offer clients a wide-ranging, single platform of financial lines insurance products. Ryan Financial Lines brings together the Management and Professional Liability talent at Ryan Specialty Underwriting Managers to provide greater synergies and efficiencies that further enhance risk management solutions and services for our clients and carriers. This unified approach brings together our expansive network of expertise with more than 70 teammates located across key territories, including North America, United Kingdom, Europe and Latin America.

ryanfinlines.com

US: RFL-US-Cyber@ryanfinlines.com | International: RFL-UK-Cyber@ryanfinlines.com