Finance industry: Top vulnerabilities in 2024 and what to watch for in 2025

BY JENNIFER CHANEY · FEBRUARY 27, 2025 · LAST UPDATED ON JANUARY 2, 2026

What you will learn

- **Which cybersecurity vulnerabilities have been most prevalent in financial services in 2024**, including information disclosure, injection bugs, and ransomware threats.
- **Why these specific weaknesses matter to financial organizations and how they are exploited in real world incidents**, helping you understand both technical and business impact.
- **What emerging threats and security trends to prepare for in 2025**, such as AI driven social engineering, advanced ransomware tactics, and evolving identity theft strategies, and how to strengthen your cyber defenses accordingly.

The financial services industry continues to be hit hard by malicious actors, with the average cost of a data breach in the sector increasing to **$6.08 million in 2024**, up from $5.90 million in 2023.

Given that nearly **1 in 4 financial businesses** have fallen victim to a data breach, it's no wonder that this industry has developed some of the most advanced defenses to safeguard its critical information.

Now, sprinkle in the **DORA regulation** which came into effect last month, all of a sudden financial companies within the EU have another level of complexity and standards to meet when it comes to cybersecurity preparedness.

While sophisticated attacks like ransomware and AI-driven phishing persist, data from our platform reveals that Information Disclosure and Injection vulnerabilities are not only prevalent in the industry but are being discovered by our researchers at critical and exceptional levels, often stemming from minor oversights rather than complex exploits.

In this blog we'll explore top vulnerabilities found within the financial services sector from our very own research community, as well as notable threats that were exploited in 2024. Finally, we'll share some tips on what to watch for in 2025 and how to keep your organization protected with multi-layered defense.

Information disclosure – A silent but widespread threat

Prevalence: Information disclosure vulnerabilities continue to be a significant concern in financial services, allowing unauthorized access to sensitive data without advanced hacking techniques.

Notable threat: In 2024, a major data breach affected LoanDepot, a prominent mortgage lender, exposing the personal information of **nearly 17 million customers**. Hackers accessed sensitive data, including names, birth dates, addresses, and Social Security numbers, highlighting the severe impact of information disclosure vulnerabilities.

Vulnerabilities our researchers found: A researcher on Intigriti's platform discovered that by simply altering a transaction ID in an application request, they could view other users' transactions. Similar flaws have exposed account details, transaction logs, and even credit card information.

Causes:

- Inadequate access controls on APIs and web applications
- Security misconfigurations failing to enforce proper authentication and authorization

Injection vulnerabilities – Exploiting weak input handling

Prevalence: Injection vulnerabilities arise when applications improperly handle user input, enabling attackers to manipulate requests and access restricted data.

Notable threat: In 2024, a notable injection incident involved BeyondTrust's Privileged Remote Access (PRA) and Remote Support (RS) products. These platforms contained a command injection vulnerability, identified as CVE-2024-12356, which allowed attackers to gain unauthorized access to unclassified data through compromised Remote Support SaaS instances.

Vulnerabilities our researchers found: One of our researcher's uncovered a critical vulnerability in a major banking mobile app's customer survey feature, which allowed them to manipulate backend requests and extract highly sensitive internal financial data, highlighting a disturbing lapse in the app's security protocols.

Other common injection vulnerability types in financial services:

- SQL Injection (SQLi): Injecting malicious queries to extract sensitive data from databases
- Server-Side Template Injection (SSTI): Manipulating web templates to execute arbitrary commands
- Command Injection: Executing unauthorized system commands through vulnerable endpoints

Ransomware attacks – Financial institutions are prime targets

Prevalence: Ransomware continues to impact financial firms globally, with attackers increasingly targeting critical data and demanding multimillion-dollar payouts.

Notable threat: The "Ghost" ransomware group, originating from China, has attacked financial institutions across over 70 countries, encrypting critical data and demanding payment for its release.

Mitigation Strategies:

- Implementing zero-trust security models
- Regular offline backups to prevent complete data loss

What to watch for in 2025

As we progress into 2025, the financial services industry must prepare for emerging cybersecurity challenges:

- **AI-driven social engineering:** Cybercriminals are expected to utilize generative AI to craft highly convincing voice and video phishing attacks, making fraudulent communications harder to detect.
- **Advanced ransomware tactics**: Ransomware attacks are anticipated to increase in sophistication, with attackers potentially targeting critical suppliers to disrupt interconnected financial systems.
- **AI-powered attacks**: Attackers are likely to use AI to automate attacks, create adaptive malware, and avoid traditional detection methods.
- **Identity theft evolution:** The rise of AI-generated deepfakes and synthetic identities may complicate identity verification processes, leading to more sophisticated fraud schemes.
- **Security as a customer experience differentiator**: As consumers face increasingly complex fraud, robust cybersecurity measures are predicted to become a key factor in customer trust and loyalty within financial services.

Final thoughts

While high-profile cyberattacks dominate headlines, our research shows that simple vulnerabilities like Information Disclosure and Injection attacks remain common in financial applications. Many of these flaws don't require advanced exploits—just minor manipulations in how an attacker interacts with a system.

Financial institutions must shift focus towards:

- Strengthening API security and access controls
- Implementing rigorous input validation to prevent injection attacks
- Enhancing real-time monitoring for insider threats

As the financial sector becomes increasingly digital, security teams must prioritize proactive defenses over reactive responses. Cybercriminals are evolving—it's time for financial services to do the same.

Are you part of a cybersecurity team at a financial organization and interested in learning more about bug bounty? Need support with DORA compliance? Get in touch for a free consultation with one of our experts today.

AUTHOR

Jennifer Chaney

Head of Marketing, Intigriti

REQUEST A DEMO

intigriti.com/demo

VISIT THE WEBSITE

intigriti.com

GET IN TOUCH

hello@intigriti.com