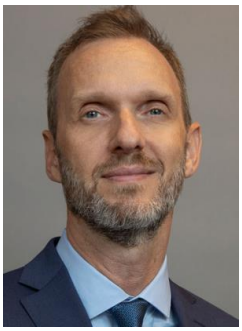
LAW360

Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Financial Cos. Should Expect More Cyber-Related Litigation

By **Peter Kamminga** (June 2, 2022, 7:12 PM EDT)



Peter Kamminga

Around the world, there is a continuing stream of cyberattacks on banks and financial institutions followed by litigation.

Two parallel developments — more stringent regulation and the move into crypto by large financial institutions — may deepen this trend in the financial industry.

Regulatory bodies such as the Federal Trade Commission, the Federal Deposit Insurance Corporation and, as of late, the U.S. Securities and Exchange Commission are focusing their efforts on containing the fallout from cyberattacks by calling for more rigid incident reporting obligations.

And, at the same time, the financial sector is rapidly expanding with fintech developments, such as Goldman Sachs Group Inc. offering its first bitcoin-backed loan in April.

All the ingredients for a perfect storm formed by the combination of increasing cybersecurity incidents, ever more stringent rules, consumer demand for frictionless transactions, evolving technologies, cryptocurrencies and harder-to-detect attacks explains the sector's current — and likely future — sensitivity to cyberattacks, regulation and persistent litigation.

Why the Financial Sector?

Why is the financial sector attracting cybercriminals? Answers lie in the maximization of funds taken and personal data when hacking.

According to a Verizon Communications Inc. report from 2020, around 86% of all cyberattacks are financially motivated. Objectives include obtaining passwords, accessing or redirecting funds, enabling identity theft and holding data hostage or selling it on the dark web.

Cybercriminals gain access to financial institutions through business email compromise, phishing, spear phishing and denial of service. DoS allows attackers to plant malware and steal data or login credentials.

The numbers show they are successful at it: Hacking and malware account for 75% of breaches in the financial services industry, and malicious software — ransomware, viruses and malware — incidents have increased by more than 90% since the first half of 2021.

Experian Information Solutions Inc.'s 2020 breach at its South African office impacted 24 million customers, Equifax Information Services LLC experienced one in 2017 that impacted 147 million customers and, in 2019, 100 million Capital One Financial Corp. customers had their data breached.

What Makes the Industry Increasingly Vulnerable?

Why are breaches happening more frequently in the financial industry? Here are four reasons:

Third-Party Vendors

Across many industries, large organizations rely on smaller companies to deliver numerous services. In the financial sector, vetting, auditing and managing these smaller service providers and ensuring compliance with regulators' requirements and security standards present a staggering challenge and introduce third-party cyber risk.

Cloud Storage

Reliance on rented cloud data servers is also expected to increase attack opportunities over the next several years. Recall the massive Capital One data breach of 2019. Security risks, such as malicious behavior by insiders, are more difficult to control when data is hosted on an off-site, third-party server.

Fintech

Consumer preferences are also expanding risks. The financial industry struggles to keep pace with demand for cashless and frictionless services that let users deposit, withdraw, transfer, send, spend and invest with minimal clicks.

Users want ease and security. Offering these transactions draws companies into the zone between convenience and exposure.

Working From Home

The COVID-19 pandemic increased the need for lean transactions and exposed security gaps in financial institutions' networks. Remote work increased security risks, and contactless shopping ballooned transaction volume and helped trigger new standards and regulations.

What is the Impact of Regulation?

The regulators' reach is expanding, and enforcement actions are on the rise. The response of regulators to the hackers' activity has been to step up their efforts.

Around the globe, they are raising expectations and holding organizations to higher standards regarding using and protecting personal data. This results in stricter regulations and more scrutiny, to include nonbanks in their widening reach and updated reporting guidelines.

Moreover, the regulators have shown that they are willing to pursue enforcement actions, thus increasing the amount of litigation against financial institutions.

Increasing Size, Scope, Scrutiny and Geographic Reach

In addition to existing laws, such as the EU's General Data Protection Regulation, the financial industry has been saddled with regulatory oversight by the SEC, the Federal Financial Institutions Examination Council, the FTC and the Federal Communications Commission. As scrutiny of cybersecurity measures increases, regulators are growing more aggressive in asserting jurisdiction over their regulated entities' cybersecurity matters.

In the new regulatory landscape, companies can trigger punitive action without a data breach. In October 2020, the U.S. Office of the Comptroller of the Currency fined Morgan Stanley & Co. LLC $60 million for its failure in 2016 to properly decommission hardware containing wealth management data at two of its U.S. data centers.

The OCC fined Capital One $80 million for failing "to establish effective risk assessment processes" when migrating operations to a public cloud environment and for failing "to correct the deficiencies in a timely manner."

Targeting Nonbanks

The Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010 gives the Consumer Financial Protection Bureau far-reaching authority as regulator of consumer financial practices, and an expansion of nonbank supervision and examination based on risk.

Payment system providers, "buy-now, pay-later" providers, medical debt collectors, debt relief services providers and lead generators may soon have to comply with these regulations, in addition to federal financial law. The CFPB has already announced that it will examine nonbank financial companies that pose risks to consumers.

Updated Reporting Guidelines

Earlier and more rigid incident-reporting obligations are the latest move of regulators attempting to further enhance cybersecurity protections.

Old FDIC and OCC reporting obligations required that notification occur as soon as possible. New guidelines direct companies to notify customers within 36 hours when they determine an incident that affects services for four hours or more has occurred.

The FTC proposed a rule that would require financial institutions to notify them within 30 days of discovering a data breach affecting or reasonably likely to affect at least 1,000 consumers. Under the regulation, financial institutions would have to ensure that they comply and transmit these reporting obligations to their external service providers.

The Cyber Incident Reporting for Critical Infrastructure Act, signed into law in March, requires entities in a critical infrastructure sector — which can include financial institutions — to report to the Cybersecurity and Infrastructure Security Agency certain cyber incidents within 72 hours and ransomware payments within 24 hours of the payment.

As these regulations trickle down, financial institutions may have to consider adopting new rules, such as requiring 24- to 36-hour reporting for all of their service providers.

How Does This Translate in Litigation?

Private litigation is expanding, and new trends are emerging. The focus on regulation and fines leads to litigation by private parties — including major class actions — and an expansion of the group of liable parties, and keeps moving into new areas with new liability questions.

Regulatory actions often trigger civil litigation. In December 2021, Capital One agreed to pay $190 million to settle a class action for its 2019 data breach on top of the $80 million settlement it reached with the OCC for the same breach one year earlier.

Data and privacy breaches have been a major growth area in class actions over the last few years. Plaintiffs counsel, consumer associations and privacy activists have turned to exploring the boundaries of group actions and challenging existing privacy legislation.

Many of the actions test new theories on standing and liability. Negligence remains a preferred theory in 50% of these cases. Others focus on breach of implied contract, violation of statute and tort-based claims.

The number of potentially liable parties is also growing. A cybersecurity breach that can be linked to inadequate internal security systems could expose financial institutions and the officers of private entities to liability. Plaintiffs could accuse the officers of breaching statutory and general law duties to act with care, skill and diligence, as well as in the best interests of the company.

Following the innovation in the financial industry, this litigation trend will likely also expand into the new areas of fintech — including cryptocurrency, nonfungible tokens and the use of smart contracts — as decentralized autonomous organizations evolve.

Celebrities, companies, countries and banks — JPMorgan Chase & Co. and HSBC Holdings PLC — are operating or buying real estate in the metaverse, where a breach may be even more damaging both financially and reputationally. Growth in these virtual activities will introduce novel privacy, security and liability issues. The collection, storage and use of biometric information may also trigger litigation.

What Does This Mean in Terms of Costs?

Cyber-related litigation is disruptive and challenging to resolve. To add insult to injury, the costs of cyber-related litigation are not only substantial, but they can also increase the extent of the fallout from an attack. There are costs in terms of disruption, damaged trust and uncertainty that come with technological and legal innovations.

The Increasing Cost of Disruption

The costs associated with being the victim of a cyberattack and the resulting disputes or litigation are substantial. The full financial impact includes data exposure, business disruption, revenue losses from downtime, notification costs, reputational damage and customer attrition.

Disputes with business partners over a data breach can disrupt normal operations. Liability and litigation risks and costs can pile up quickly. A process that drags on invites unwanted attention and requires more money.

Litigation costs and settlements can exceed the damage caused by the data breach itself. A business that needs to resume normal operations should prioritize expeditiously resolving a matter.

Trust and Reputational Effects

Trust and security are critical in the financial sector. A breach at the main organization or one of the supporting service companies can drive away customers, contract partners and third parties interested in repeat business.

Adverse cyber events create the kind of exposure that chips away at consumer trust and security and disrupts relationships among business partners. Despite precautions and complex layers of security, only about 0.05% of cyber events are prevented. Early detection and damage control are therefore key.

Taking swift action and resolving litigation quickly and in a manner that minimizes damage and exposure benefits the company's reputation and ability to do business.

Technological Aspects

As technologies advance, lawyers and neutrals — judges, arbitrators — are tasked with understanding the complex technical concepts underlying cases. Litigating these matters challenges lawyers and neutrals to interpret novel incidents under existing laws. Without proficient understanding of the technology, litigating and ruling can prove challenging.

Considering the costs of litigation, there may be a benefit to limiting the length of litigation and attempting to reach a resolution.

Takeaways and Outlook

Increasing attacks, significant breaches and large fines or settlements justify the anxiety a recent Allianz survey reported across the financial services world. Even as institutions fortify their cybersecurity efforts, industry trends are creating new entry points for increasingly hard-to-detect attacks.

With bad actors already focused on the sector, increasing use of third-party providers and cloud storage, shifting consumer demands and the fallout from the pandemic are exacerbating risks. The regulators are stepping up their efforts and ready to enforce.

These developments make the industry more vulnerable to hacking and regulatory and civil litigation, and protracted litigation compounds the costs of the fallout, as it impacts finances, trust and reputation, hurting both institutions and their clients. As a result, the financial sector will likely remain among the sectors most prone to cyber-related litigation.

Settling disputes early on serves consumers, the original victims and the financial industry.

Peter Kamminga is a mediator at JAMS.