CARLTON FIELDS

Increasing Risks and Regulations: 2024's Key Cybersecurity, Privacy, and Data Rights Developments

By: Trish Carreiro, Carlton Fields, P.A.

ALI CLE Life Insurance Company Products 2024

New technologies and new implementations of existing technologies captivated the life insurance industry's attention throughout the past year and thrust data, and the associated privacy and cybersecurity issues involved in the collection, use, transfer, storage, and disclosure of such data, into the spotlight. This paper provides an overview of some of 2024's key privacy and cybersecurity developments affecting the life insurance industry.

I. The Threats Continue

From service provider breaches to SIM swapping to ransomware, cybercriminals have continued their malicious efforts throughout 2024. In the first half of 2024 alone, federal agencies issued over 20 cybersecurity advisories, including, advisories regarding:[1]

- A critical vulnerability in the MOVEit Transfer, Secure File Transfer Protocol (SFTP) Module that could lead to authentication bypass.[2] A new patch mitigated the vulnerability, but the threat spurred fears of a potential repeat of 2023's widespread MOVEit compromise.
- Ransomware groups like Black Basta,[3] Akira,[4] and Phobos.[5]
- A new malware known as Androxgh0st, which targets files with confidential information.[6]

In a recent report to the NAIC's Cybersecurity Working Group, the FBI's Internet Crime Complaint Center ("IC3"), reported an increase in cybercrime losses and the prevalence of ransomware, phishing, and spoofing attacks. According to a recent NAIC report on the cyber insurance market, between 2022 and 2023 cyber insurers have seen a 20% increase in the number of claims from businesses earning more than $100 million and a 72% increase in claims severity for the same

---

[1] *See* Mark Rosanes, *The Insurance Industry Cyber Crime Report: Recent Attacks on Insurance Businesses*, INS. BUS. https://www.insurancebusinessmag.com/us/guides/the-insurance-industry-cyber-crime-report-recent-attacks-on-insurance-businesses-448429.aspx#:~:text=In%20a%20notification%20letter%20dated,personal%20information%20accessed%20by%20hackers (published in 2023, but updated throughout 2024).

[2] Financial Industry Regulatory Authority (FINRA), *Cybersecurity Alert: FINRA Notifies Member Firms of MOVEit Software Vulnerability (CVE-2024-5806)* (June 27, 2024), https://www.finra.org/rules-guidance/guidance/cybersecurity-alert-moveit-software-vulnerability-cve-2024-5806.

[3] CISA, *#StopRansomware: Black Basta* (May 10, 2024), https://www.cisa.gov/news-events/cybersecurity-advisories?f%5B0%5D=advisory_type%3A94.

[4] CISA, *#StopRansomeware: Akira Ransomware* (Apr. 18, 2024), https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-109a.

[5] CISA, *#StopRansomware: Phobos Ransomware* (Feb 29, 2024), https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-060a.

[6] CISA, *Known Indicators of Compromise Associated with Androxgh0st Malware* (Jan. 16, 2024), https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-016a.

group over that time. Technology has helped fuel the growing threat environment as its strength is manipulated by criminals for their own gain.

II. Technological Opportunities Bring Risks and Rewards

Technology offers insurers much promise. Among many opportunities, it can help with collecting and analyzing valuable data, expanding product offerings, and streamlining customer service and underwriting processes. But it also comes with risks, not the least of which are the many privacy and cybersecurity challenges involved. Some of the technologies that have captivated the industry's imagination throughout the last year include artificial intelligence, cloud computing, connected devices aka internet of things ("IoT"), and smart contracting/blockchain. Key cyber and privacy risks involved in these technologies are discussed briefly below.

A. Artificial Intelligence

Artificial Intelligence ("AI") has almost limitless potential to impact the insurance industry by enhancing insurers' capacity to collect and analyze large datasets. With the help of AI algorithms, insurers can leverage these large datasets to identify patterns, assess risks, set premiums, design personalized policies, and more generally promote efficiency, flexibility, personalization, and cost-savings. Generative AI has drawn considerable attention (and adoption) for its capabilities improving customer service via chatbots to answer customer questions, routing calls, or assisting insurers in responding to customer questions.

While insurers can no doubt benefit from AI integration, it also presents cybersecurity and privacy risks. On the privacy side, consideration must be given to the sheer volume of data needed to fuel these technologies, the underlying notices and consents regarding the collection and use of such data, and the litigation risk created by plaintiffs' interpretation of the law as applied to these technologies. On the cybersecurity side, AI programs can be vulnerable to adversarial manipulation and weaponized by threat actors to cause data breaches. These risks are particularly pronounced if the AI program is used to manage personal information or make decisions that affect an individual's access to essential services. Even when personal information is not involved (i.e., the data is not linkable to a particular person, household, or device), expanding notions of entitlement to controlling individuals' data, even if not linked to them, has led to litigation. Recognizing the cyber risks inherent in AI, the NY Department of Financial Services ("NY DFS") recently published guidance meant to explain how covered entities can use the NY DFS Part 500 cybersecurity framework to address cyber risks arising from AI. According to the guidance, AI increases the possibility for AI-Enabled social engineering, supply chain vulnerabilities, and exposure or theft of large quantities of nonpublic information necessary to fuel AI technologies. As a result, NY DFS stresses the importance of risk assessments and risk-based policies and procedures, third-party service provider and vendor management, access controls, employee training, monitoring, and data management.

B. The Cloud

Cloud computing can provide a centralized, scalable, and cost-effective method of storing data, allowing insurers to store data more cheaply and access it more easily. This data can then be harnessed and used, including to fuel emerging technologies, like AI.

Despite its benefits, cloud computing can create complexities that make identifying and addressing security risks more difficult and inadequate backup or recovery contingencies can intensify the impact of any particular data incident (i.e., the compromise of a single cloud computing service provider could domino throughout the industry). Furthermore, these services' large pools of data could attract more attention from data thieves. Contractually, these service contracts often include low limitations of liability, making the importance of negotiated carve outs to these limits particularly important for managing risk.

C. Connected Devices/IoT

Connected devices, like health and fitness wearables, allow insurance companies to collect and analyze vast, valuable datasets that provide real-time insights into individuals' health, habits, and risk-levels, allowing more personalized and accurate risk-assessments and customized policies, opportunities for preventative treatment, and the potential for more effective wellness incentive programs. These devices and the associated mobile and web applications that store the data collected by these devices, however, are sometimes prone to weak security or authentication requirements. For example, these devices often have low processing power. Low processing power reduces costs and extends battery life, but also limits the device's capability to support cybersecurity measures like firewalls. Additionally, the connected nature of these devices means that compromising a single device can serve as a gateway into compromising an entire network of devices. From a privacy perspective, this sort of passive collection and use of vast amounts of sensitive data raises heightened concerns regarding transparency and appropriate notice and consent.

D. Smart Contracts and Blockchain Technology

Smart contracts and blockchain technology can help insurers streamline claim management and adjudication and can provide a transparent, tamper-proof way to collect and store customer information.[7] At their best, these technologies can enhance network security, but they too come with certain risks, such as:

- Their reliance on immutable records can complicate efforts to respect privacy rights (e.g., rights of correction or deletion) and fix embedded coding errors or bugs discovered after adoption to the network;
- If relying on external code or data, those can be corrupted and compromise the technology's integrity; and

[7] Aditya Kathpalia, *7 Ways Insurance Technologies are Transforming Life Insurance Lifecycle*, DAMCO (Mar. 24, 2023), https://www.damcogroup.com/blogs/how-insurance-tech-transforming-life-insurance-lifecycle. *See also* Gina Alsdorf and Jason Berkun, *Is blockchain the next big thing for insurance companies?*, Reuters (Oct. 9, 2024 9:20 AM EDT), https://www.reuters.com/legal/legalindustry/is-blockchain-next-big-thing-insurance-companies-2024-10-09/.

- They can be exploited for unauthorized access and manipulation.

All the preceding are examples of the many risks and opportunities involved in the insurance industry's increasing utilization of technology. The troves of data underpinning and proliferating from these technologies are valuable assets that create immense opportunity, but also invite increasing scrutiny. The more valuable the data and its uses, the greater then incentive to create and collect the data, and the longer it is stored, the greater the risk that the data may be compromised or the uses for such data evolve over time to differ from those uses/disclosures initially disclosed to customers and the public.

III. Increasing Regulations, Enforcement Actions, and Private Litigation

From AI bulletins to increasing cyber disclosures and regulations and active private litigation where private plaintiffs bring putative class actions alleging violations of decades' old privacy statutes by new technologies, the promise of new technologies can, if not appropriately managed and implemented, result in substantial losses.

Regulators have responded to increasing cyber risks by updating their regulations, urging increased cybersecurity readiness through guidance documents, and increasing their cyber enforcement, investigations, and penalties. NY DFS, for example, after releasing its second amendment to its cybersecurity regulations (Part 500), settled alleged violations of its Part 500 with a large insurance company following a cybersecurity breach resulting from a vulnerability in a proprietary software application.

On May 16, 2024, the Securities and Exchange Commission announced that it had adopted amendments to Regulation S-P ("Reg S-P") to modernize and enhance the protection of consumers' nonpublic personal information.[8] The SEC fact sheet for these amendments is attached as Appendix 1. The amended rule expands the entities and data subject to Reg S-P and creates new obligations for covered institutions. The revised Reg S-P applies to broker dealers (including funding portals), investment companies, registered investment advisers, and transfer agents[9] (collectively, "covered institutions.").[10] Larger entities must comply with the amended rule by December 3, 2025, while smaller entities will have until June 3, 2026.[11] To comply with the revised Reg S-P, covered institutions must:

1. **Adopt a written incident response program ("IRP").** The IRP must be reasonably designed to detect, respond to, and recover from unauthorized access to or use of customer information.[12] This IRP must include policies and procedures to:

---

[8] *See* SEC, *SEC Adopts Rule Amendments to Regulation S-P to Enhance Protection of Customer Information*, (May 16, 2024), https://www.sec.gov/news/press-release/2024-58.
[9] *Id*.
[10] *Id.*
[11] *See Id.*
[12] Regulation S-P: Privacy of Consumer Financial Information and Safeguarding Customer Information, 89 Fed. Reg. 47688, 47692 (June 3, 2024).

- assess the nature and scope of any incident involving unauthorized access to or use of customer information;

- take appropriate steps to contain and control the incident; and
- notify individuals if their information was, or is reasonably likely to have been, accessed or used without authorization, unless the information involved is not reasonably likely to be used in a manner that could cause substantial harm or inconvenience. This must be done "as soon as practicable," but no later than 30 days after becoming aware that unauthorized access to or use of customer information has occurred or is reasonably likely to have occurred.[13]

Covered institutions may only delay notification beyond 30 days if the Attorney General informs the SEC in writing that the required notice would pose a substantial risk to national security or public safety.[14]

2. **Oversee service providers.** Covered institutions must establish, maintain, and enforce written policies and procedures reasonably designed to ensure oversight of service providers, including to ensure that affected individuals receive any required notices.[15] This includes ensuring service providers take reasonable measures to protect against unauthorized access to or use of customer information and provide notification to the covered institution as soon as possible, but no later than 72 hours after becoming aware that a breach in security has occurred.[16]

3. **Safeguard and dispose of NPI appropriately.** Covered institutions that receive nonpublic personal information from their customers (including customers of other financial institutions) must comply with expanded safeguards and disposal rules and document **compliance with the same.**[17] The required retention period for these records varies by entity type so covered institutions review and potentially revise their record-keeping practices, including their document retention and deletion policies and examination preparations.

The revised Regulation S-P does, however, come with some good news: it codified the FAST Act exception to Regulation S-P's annual reporting requirements,[18] meaning that the revised regulation does not require covered institutions to mail an annual privacy notice if the institution's data practices do not trigger opt-out rights and its policies and practices have not changed from its most recent disclosure to customers.[19]

Some practical, potentially unintended, consequences of these revisions include:

---

[13] *See id.*
[14] *Id.* at 47757.
[15] *Id.* at 47691.
[16] *Id.* at 47706.
[17] *Id.* at 47697.
[18] *Id*. at 47723.
[19] *Id.*

1. The 72-hour notice requirement for service providers to notify covered institutions of a breach may actually be longer than what institutions' contracts with customers currently provide. In our experience, many parties have typically settled upon 48 hours (rather than 72 hours) for such notifications.

2. Rising disclosures and requirements surrounding cyber incidents necessarily increase litigation risk, giving plaintiffs further fodder for feeding frenzies after any incident.

The revision's use of a 72-hour notification requirement may also signal that the SEC has reconsidered the 48-hour notification period included in its proposed rules relating to cybersecurity risk management for investment advisers, registered investment companies, and business development companies, which had drawn significant blowback from the industry. The proposed rules would, among other things, require investment advisers and funds to implement written cybersecurity policies and procedures, disclose significant cybersecurity risks and incidents that affect clients and shareholders, and comply with new recordkeeping requirements. The comment period on these proposed rules closed in May 2023 and final action is still pending.

The NAIC for its part, is continuing its work to develop a new privacy model. Although the Working Group had created a draft model, Model 674, the group chose to put that draft aside and is currently beginning its revisions to Model 672 anew. It will likely be some time until a new privacy model is ready for adoption.

Although thanks to entity-level Gramm-Leach-Bliley Act exemptions, life insurers have remained largely exempt from the onslaught of state comprehensive privacy laws, they have not escaped private litigation. Privacy-related class action litigation escalated in 2024, with insurers facing many variations of the same tune: plaintiffs' weaponizing decades' old privacy statutes that include private causes of action and statutory damages to allege that new technologies offend such laws. While the industry has been able to deliver some swift blows to some theories (e.g., Illinois's Genetic Information Privacy Act), insurers still face increased litigation risk surrounding their use of technology.

IV. What Can Be Done?

Some risk-reducing measures to consider:

- **Annual Maintenance.**
    - **Refreshing existing data maps** to reflect changes from throughout the year and planned forthcoming changes can be a helpful first-step for understanding practices and permitting informed compliance programs and risk evaluations.
    - **Ensuring compliance** with the latest laws and regulations and industry practices (e.g., NIST Cybersecurity Framework 2.0 or CISA Cybersecurity Performance Goals). Given the year's developments, this may include steps such as preparing

for NY DFS Part 500 compliance and associated filings, developing or revising an incident response plan, revising privacy notices, evaluating vendor contracts, etc.

- **Before implementing a technological solution:**

    - **Begin with a problem.** The marketplace is replete with vendors seeking to sell solutions, but not all technologies are equally valuable, and they can create unnecessary legal risks. Defining a specific problem can help prioritize and evaluate technological solutions.

    - **Consider all potential solutions, the risks involved in each, and how to counter or limit them.** This includes a hard look at the underlying data involved, the risks associated with any particular use case, and steps that could be taken to reduce risks. Understand the technology, the problem it is being used to fix, data flows, the use case, and resulting obligations and risks (e.g., contractual, regulatory, and private litigation).

- **Plan for change.** Privacy notions (e.g., expectations regarding transparency, level of consent, data choice, and data minimization) may be shifting. Some practices that are technically permitted may still not be worth the litigation risk involved. Additionally, privacy and cyber risks are an ever-changing risk; be sure to re-evaluate them regularly.

- **Discuss risk preferences and which risks are worth taking.**

- **Consider alternative dispute resolution agreements and class action waivers.**

- **Plan (and practice) for the worst.** Technologies sometimes fail. Consider broadening (and rehearsing) your recovery and incident response plans.

APPENDIX 1