RT ProExec
INSIGHTS
VOLUME XXVIII ISSUE 4
SPRING 2025

DATA BREACH RISKS

Regulatory Environment, Claims Trends & Coverage Considerations

Data breaches make businesses vulnerable to regulatory action and class action liability risks. Companies that collect data—whether from employees or customers—need to be aware of the claims trends and coverage considerations surrounding unlawful data collection practices and data breach risks.

Data Privacy Class Action Developments

Businesses regularly collect data on everything from consumer shopping and internet browsing habits to employee identification and financial information. As data sources, collection and uses increase, so do the litigation exposures.

Businesses may face lawsuits when data is collected without consent, used improperly or exposed due to lax security standards.

What Is Unlawful Data Collection?

The term "data" can refer to any type of facts, figures or statistics that a company collects.

When businesses collect or store data in ways that violate state or federal laws, they may face accusations of unlawful data collection practices. Since laws are developing, what constitutes unlawful data collection may change rapidly.

Three Developing Litigation Exposures

1. VPPA-Based Pixel Claims. You might think that a 1988 law designed to regulate brick and mortar video rental companies would not have much relevance today. However, the Video Privacy Protection Act (VPPA), which protected the video-viewing histories of customers, is now the basis of lawsuits against modern companies offering video content. According to K&L Gates, there were more than 80 VPPA class-action lawsuits filed in 2022, many of which targeted consumer products companies, university sports programs and health services websites. The case outcomes have been mixed.

2. Pixel Tracking Claims. Many organizations use pixel tracking to track behavior and target ads, though this practice has come under fire. Multiple class action lawsuits have involved the use of Meta's tracking pixel, often claiming that the practice amounted to unlawful collection of data. Some data shared with Meta may represent a HIPAA violation. In one example, The National Law Review says Costco has been sued over its use of Meta's tracking pixel on its pharmacy website.

3. Biometric Claims. More companies are using fingerprints, facial scans and other forms of biometric data to identify customers and employees. According to Legal Dive, these techniques have triggered an increase in lawsuits using the Illinois Biometric Information Privacy Act (BIPA). BIPA went into effect in 2008, making Illinois the first state with a comprehensive biometric privacy law, although other states have enacted similar laws since them. BIPA lawsuits have increased in recent years as more companies embraced biometric data, and there have been more than 2,000 lawsuits since 2018.

CONTACT
RT ProExec
rtproexecinfo@rtspecialty.com

Or contact your local RT ProExec broker at rtspecialty.com

RT ProExec

High-profile class-action lawsuits include one against Facebook that resulted in a $650 million settlement and one against Google that resulted in a $100 million settlement. In July 2024, the Attorney General of Texas announced that he had secured a $1.4 billion settlement with Meta over the company's use of biometric data—the largest settlement ever from a class-action lawsuit brought by a single state. However, it's not just large tech companies that are vulnerable to these claims, any company that uses biometric data is at risk. For example, Kiosk Marketplace says the fast food chain Steak 'n Shake has been sued over its collection of facial recognition data via its ordering kiosks.

4. CIPA Wiretapping Claims. Beyond just video viewing behavior, pixel tracking and biometric data, any unauthorized collection of personally identifiable information (PII) or protected health information (PHI) may result in litigation. Such lawsuits are a growing risk as states pass strict data privacy laws. Plus, existing laws, such as the California Invasion of Privacy Act (CIPA), are being used in new ways.

CIPA is a 1994 law that prohibits the recording of confidential conversations without the consent of everyone involved, making California a two-party consent state. Originally, the law was primarily applied to phone calls, but as communications technology evolves, it has found new applications.

According to Nixon Peabody, there has been a flood of CIPA litigation. Even companies that tried to be diligent about creating compliant privacy policies are getting hit with lawsuits accusing them of aiding wiretapping due to the use of third-party technology. For example, The National Law Review reported Domino's Pizza, Inc. and ConverseNow Technologies, Inc. have been sued over the use of ConverseNow's Voice AI technology, which records and analyzes customer data to process orders and suggest additional items. Furthermore, the American Bar Association states some new CIPA cases have focused on website tracking technology, alleging that they record interactions and therefore amount to unlawful pen registers.

Final SEC Cybersecurity Disclosure Rule

As cybersecurity threats proliferate, the SEC has sought to protect investors. This approach has led to a final cybersecurity disclosure rule, which was adopted in 2023.

This rule creates two new requirements for public companies:

- Within four days of determining that a cybersecurity incident is material, public companies must disclose it.
- On an annual basis, public companies must disclose information regarding cybersecurity risk management, strategy and governance.

An incident is material if a reasonable investor might consider it important when making an investment decision. To determine whether an incident is material, companies should apply the same considerations they would use for other types of events.

These disclosure requirements will give investors consistent and comparable disclosures that can be used to evaluate companies. However, the disclosures may also give government agencies and plaintiff lawyers more opportunities to find fault with a company's cybersecurity practices, leading to increased liability.

CONTACT
RT ProExec
rtproexecinfo@rtspecialty.com

Or contact your local RT ProExec broker at rtspecialty.com

RT ProExec

How can companies prepare for increased scrutiny?

- Embrace transparent, proactive cybersecurity risk management at the upper levels of a company. Management and board members can oversee cyber risks in a real and robust way.
- Consider how internal communications might be perceived by outsiders. Internal communications, especially among security teams, should maintain appropriate and mature tones when discussing cyber risks.
- Foster collaboration between the teams working on SEC disclosure documents and the teams responsible for the company's cybersecurity risk management.

Risk Management Strategies

Businesses in all industries are leveraging innovative technologies to improve customer service, increase sales and optimize operations. However, these technologies tend to necessitate the collection of data. Both consumers and lawmakers are increasingly concerned about what happens to this data. It's important to be mindful of the risks and implement appropriate risk management strategies.

- **Consider both old and new legislation.** According to the IAPP, state-level privacy legislation has become increasingly robust since the California Consumer Privacy Act (CCPA) was enacted in 2018. In 2024, 41 bills were considered and 7 were enacted. However, recent lawsuits involving the California Invasion of Privacy Act and the Video Privacy Protection Act prove it's not only new legislation that companies need to watch out for—old rules designed to protect data privacy are being applied to emerging technologies.
- **Be proactive.** Periodic cybersecurity risk assessments can help companies stay ahead of problems and bolster their cyber risk management strategies as needed. Regular audits and strong compliance are key.
- **Ask about the board's cyber oversight process.** Consider whether another in-house cybersecurity expert on the board could be in the shareholders' best interests.
- **Focus on transparency and consent.** It's important to be compliant with the details of any applicable legislation regarding data privacy. Such laws may have specific requirements, such as the CPPA's requirement that companies respond to requests to delete, correct or identify personal information within 45 calendar days.
- **Respond to incidents thoroughly and promptly.** If a data breach occurs, a prompt response will help businesses contain the damage and minimize liability. The response will need to comply with relevant state data breach notification requirements. Additionally, the SEC has adopted rules that require public companies to disclose certain cybersecurity incidents. Failure to comply with notification rules could result in large penalties. For example, the SEC says it levied a $10 million penalty against The Intercontinental Exchange, Inc. over the failure of nine wholly-owned subsidiaries to inform the SEC of a cyber intrusion in a timely manner.
- **Secure cyber insurance with data breach coverage.** Cyber insurance covers many of the costs associated with a data breach and facilitates a response that minimizes the risks. However, each cyber policy provides different coverage.

CONTACT
RT ProExec
rtproexecinfo@rtspecialty.com

Or contact your local RT ProExec broker at rtspecialty.com

RT ProExec

Data Breach Coverage Considerations

Whether a cyber insurance policy provides coverage in specific instances will depend on its terms. When comparing data breach coverage options, consider these issues:

- **How does your policy address wrongful collection?** Does the policy provide affirmative coverage or is the policy silent regarding the exposure? Or is the risk excluded?
- **Do you have coverage for defense and indemnity?** For example, if your policy provides affirmative wrongful collection coverage, is the coverage limited to defense costs only or is coverage also extended to other indemnification costs?
- **How does your policy address litigation trends?** Consider VPPA, pixel tracking technology, BIPA, CIPA and other unauthorized collection claims. Is coverage provided, excluded or is the policy silent?
- **Do you have coverage for defense, fines and penalties stemming from failure to report?**

Have questions?

Our team can help you understand the ins and outs of data breach coverage options to ensure your clients have the most robust protections in place.

CONTACT
RT ProExec
rtproexecinfo@rtspecialty.com

Or contact your local RT ProExec broker at rtspecialty.com