Compliance, Privacy and State Law Whack-A-Mole

By Dara Tarkowski and James Ward

This article is an excerpt from the Spring 2023 RMAI Digital Dispatch *(pages 14 and 15), originally published April 3, 2023.*

The financial sector is one of the most data-driven industries, with companies collecting and managing vast amounts of personal and financial data. As a result, privacy laws like the California Consumer Privacy Act (CCPA, which was recently amended) and the now-active Virginia Consumer Data Privacy Act (VCDPA) and Colorado Consumer Privacy Act (ColCPA) are of utmost importance for companies in the financial sector, particularly those buying, selling, managing and servicing receivables.

Here, we will explore the importance of state privacy laws for accounts receivables management (ARM) companies and discuss how to approach compliance with these regulations to protect consumers' personal and financial data.

Since the entire industry became light-headed holding its collective breath for federal privacy regulation, we have finally come to grips with the fact that federal privacy legislation isn't going to relieve us of our state obligations any time soon. As the International Association of Privacy Professionals (IAPP) observed, "Congress, industry, civil society and the White House have all taken steps toward the creation of a U.S. federal privacy law. What this law will look like — and when and if it will happen — are still very much in question, but day-by-day it's looking more likely that a federal law is in the United States' future." These authors are not holding our breath.

What does that mean? State privacy laws are critical because they establish new requirements for the governance and oversight of consumers' personal and financial data. Existing laws like Gramm–Leach–Bliley Act (GLBA) or Health Insurance Portability and Accountability Act (HIPAA) may be familiar to us, but they're of comparatively narrow scope and are poorly understood, especially by non-specialists. State privacy laws like CCPA, on the other hand, are far more wide-ranging and they've captured public attention, not least because consumers have become increasingly concerned about how their data is being used and shared.

Generally, state privacy laws in the United States provide consumers with the right to know what personal and financial data companies collect about them, the right to request that companies delete their data, and the right to opt-out of the sale of their data.

For companies handling substantial amounts of consumer financial or borrowing data, compliance with these laws is crucial because they handle some of the most sensitive personal and financial information. These laws provide a framework for companies to follow when collecting, storing, and sharing this data, and they can help protect both the company and its customers.

ARM companies (like all financial institutions) must comply with the CCPA and other state privacy laws. Compliance requirements may vary depending on the company's size, scope, and data management practices. On the less intense side, laws like VCDPA and ColCPA require companies to disclose what personal and financial information they collect and how they use it. They must also provide consumers with the right to opt-out of the sale of their data and the right to request that their data be deleted. Additionally, companies must implement reasonable security measures to protect the data they collect.

The CCPA is similar to these laws but is more demanding in that it requires companies to disclose what data they collect and how they use it. CCPA goes further, as well, by requiring companies to obtain consent from consumers before collecting their data and to allow consumers to correct inaccurate data. The CCPA is also actually being enforced. On January 27, 2023, ahead of Data Privacy Day, California Attorney General Rob Bonta announced "an investigative sweep, sending letters to businesses with mobile apps that fail to comply with the California Consumer Privacy Act (CCPA). This year's sweep focuses on popular apps in the

retail, travel, and food service industries that allegedly fail to comply with consumer opt-out requests or do not offer any mechanism for consumers who want to stop the sale of their data. The sweep also focuses on businesses that failed to process consumer requests submitted via an authorized agent, as required by the CCPA." (https://oag.ca.gov/news/press-releases/ahead-data-privacy-day-attorney-general-bonta-focuses-mobile-applications%E2%80%99)

It would be easy to assume that the traditional carveouts and exemptions for data obtained pursuant to GLBA or FCRA continue to apply, and that the sector-based data management requirements of the past thirty years will continue apace. That would be a mistake.

CCPA contains an exemption for data that is, itself, "subject to" GLBA or Fair Credit Reporting Act (FCRA) and is excluded from the general requirements of the law. This means that any data which is not itself, for example, covered by GLBA as related to consumer financial activities subject to CCPA – and your organization has more of it than you think. This also creates an interesting scenario. If a company has an email address of a California resident that it obtained through processing a financial transaction (or was provided by the originating creditor who processed the financial transaction), that data would be subject to the GLBA exemption. But if that same company obtained the email address by purchasing it from a data broker or skip tracing company, the exemption doesn't apply, because that particular data is not subject to GLBA. Even more concerning: even if data is subject to GLBA, if there is a data breach and data is lost or disclosed, the exemption does not apply, and California residents can sue in a private cause of action with statutory damages. We have already seen this begin.
Clearly, for financial sector companies managing receivables, compliance with these laws can be particularly challenging. Receivables management necessarily involves vast volumes of data in order to establish both consumer profiles and their related financial data. Because regulators, especially in California and New York, have taken an aggressive stance on the management and oversight of financial data, it is essential for the ARM industry to develop comprehensive privacy plans and, more importantly, implement them.

How?

- Implement data inventory and mapping procedures to understand what data is being collected, where it is being stored, and how it is being used. Ask yourselves. Why do I have this data? Do I have a business use? If not, do I actually need it? How can I align my goals with the retention requirements that the law requires, and that my clients and partners require by contract?

- Implement reasonable security measures to protect the data collected, including encryption, access controls, and data breach response plans. Most ARM companies have a solid grip on this, particularly RMAI certified companies!

- Provide consumers with a way to request access to their data, correct inaccurate data, and delete their data, assuming the data is not otherwise GLBA or FCRA exempt.

- Train employees on data privacy policies and procedures to ensure that they understand their responsibilities when collecting, storing, and sharing data. When, if ever, has your company conducted a tabletop exercise or engaged an expert to test your employees' knowledge, awareness and judgment?

For companies managing receivables, compliance with state privacy laws can be particularly challenging. But taking steps now -- with the advice of experts -- can prevent substantial downside risk in the future. And, given that privacy laws are proliferating across the country, there is every reason to believe that even in states without a privacy law today, the circumstances will be different very soon.

Dara Tarkowski
Founding Partner
Actuate Law, LLC

Dara Tarkowski is a renowned legal expert shaping the future of law, technology and highly regulated industry. As a published author, keynote speaker, and the co-founder of Actuate Law and the reg-tech start-up quointec, she is an outspoken voice on how technology is impacting the future of delivering legal and compliance advice to financial services companies.

James Ward
Special Counsel
Actuate Law, LLC

James is a data strategist, privacy lawyer, litigator and author. In addition to his role with Actuate, James is the founder and managing partner of Ward PLLC, a data strategy consultancy and privacy firm. He advises clients on how to create and market valuable data products and how to manage complex privacy and data protection requirements, including GDPR, HIPAA, and CCPA.