Featured Professionals

Sten-Erik Hoidal, CIPP

Latest Privacy Laws Provide Expanded Protections

Legal Update
09.04.2018

Community banks are no strangers to privacy and data security laws. The Gramm Leach Bliley Act (GLBA), for example, requires banks to give customers notice regarding the bank's privacy policy and to allow customers to opt out of having their information shared for marketing purposes. Certain other industries, such as healthcare companies, are similarly used to complying with privacy law requirements. The latest trends in privacy laws, however, are not limited to certain industries, and they include privacy rights for consumers that could have a significant impact on how companies treat customer information.

In 2016, the European Union (EU) adopted the General Data Protection Regulation (GDPR) to provide its residents with expanded privacy rights. The new law became effective May 25, 2018. At first glance, many U.S. community banks may have dismissed this new law because they do not do business in the EU. However, the GDPR is worth a second look both because of its potentially broad reach to non-EU companies and because some of the rights it affords EU consumers have been replicated in another new law enacted closer to home: the California Consumer Protection Act of 2018 (CCPA) enacted on May 25, 2018, and effective January 1, 2020. Together, these two laws could signal a trend toward privacy and data security rights that extend beyond protections seen in current laws, such as the GLBA.

Who is subject to the EU's GDPR?

The GDPR applies to all companies "established" in the EU, as well as to those outside the EU that offer their products and services to EU residents. It also applies if a company monitors an EU resident's behavior using data it has collected (e.g., via cookies on its website). Banks that do not market, or offer goods or services, to EU residents and who do not monitor the activity of EU residents who happen to visit the bank's website may feel fairly comfortable that this law does not apply to them. But a grey area exists when a bank has one or more EU residents as customers (perhaps because they moved to the EU after becoming a customer) because by continuing the customer relationship, the bank may be considered to be offering products and services to those EU customers. When that is the case, banks should consider how to address potential GDPR compliance risks.

What does the GDPR require?

The GDPR requires companies to provide EU customers with prescribed privacy notices and to obtain customer consent or have some other appropriate lawful basis to use or share customer information. EU customers must be allowed to correct inaccurate data, and they can require the company to erase their data in some circumstances. Further, upon request, the company must provide customers with copies of their data in machine-readable format. The law includes data security standards and a requirement to make notifications within 72 hours of a security breach. Other obligations include contractual requirements for relationships with third party data processors, record retention obligations, and restrictions on transfers of personal data outside the EU. EU residents have rights to damages against noncompliant companies in some cases. EU regulatory agencies can also take action, including levying fines for noncompliance up to €20 million or 4 percent of a company's annual global revenue, whichever is higher.

Who is subject to the CCPA?

California's new CCPA takes a different approach to determining which companies must comply, but it applies some of the same new privacy rights to California residents. The CCPA applies to for-profit companies collecting personal information from California residents that annually (1) have gross revenue of more than $25 million; (2) receive, buy, sell, or share personal information on at least 50,000 consumers, households, or devices; or (3) derive at least 50 percent of their revenue from selling consumers' personal information.

What does the CCPA require?

CCPA compliance includes certain opt-out rights to information sharing. This law also expands into new territory by requiring companies to erase information they have collected about consumers upon request (with various exceptions) and to ensure their third party service providers do the same. The law also gives Californians the right to receive information regarding the types of information collected and shared. Further, the CCPA provides private rights of action to customers harmed by security breaches in some cases. The CCPA does not apply to personal information collected, processed, sold, or disclosed pursuant to the GLBA, but only to the extent it is in conflict with the GLBA. The law calls for the California Attorney General to adopt implementing regulations, so further details about compliance expectations will follow.

What are some best practices in light of these new laws?

As with any new law, the first step is to evaluate its applicability to the bank. The EU's GDPR may seem unlikely to apply at first glance, but banks should review whether they have EU resident customers and whether they are offering goods or services to those customers such that they would be brought within the GDPR's ambit. If so, then the bank should determine if or how it needs to respond. It is more

likely that U.S. banks do business with California residents. Banks with California customers should consider whether the CCPA is triggered based on the bank's annual revenue, customer base, or income streams. Both of these laws reflect the increasing importance of monitoring where your customers reside, who you are marketing to, and how you are using information such as cookies to further your marketing efforts.

Regardless of whether either of these two new laws applies to your bank, undoubtedly they will apply to many regional and most or all large U.S. banks. That means many U.S. banks will comply with the new breach notification periods, data erasure requests, requests for copies of collected information, and other requirements of these new laws. And the reality is that when a subset of banks increases their consumer protection services, it can eventually raise expectations from consumers, lawmakers, and regulators that other banks do the same.

Therefore, it would be prudent to keep an eye on how compliance with these laws develops and to consider what changes your bank may need to make in the future should these or similar requirements affect you. For example, consider the various locations where customer data is stored. How easy would it be to retrieve a copy of a customer's data and provide it securely in machine readable format? As you formulate your vendor management strategy, are there vendors who would make that process easier? Ask your vendors about their readiness to comply with the standards set forth in the GDPR and CCPA. As you formulate marketing strategies, are there steps you can take to avoid unnecessary risk related to customers located in the EU or California?

Takeaway

Evolving privacy trends may lead to fundamental changes in how all community banks treat customer information. Considering these potential impacts now will help management make strategic decisions that lessen future disruption to bank operations.