THE CREDIT TIMES

CCC of New York
Serving the Credit Industry's Professionals

June 2021

A Publication of The Commercial Collection Corp. of NY, Inc.

Stricter Privacy Laws Are Here to Stay

By: Wanda Borges, Esq.
Borges & Associates, LLC

While many retail businesses closed their brick and mortar stores in the past few years, consumers have become more accustomed to purchasing goods online. Since the coronavirus pandemic began in early 2020, cybercrime has climbed and online transactions are subject to cyberattacks. Even before the pandemic, some states were taking steps to protect the personal information of consumers. So what, you may ask, does this have to do with business to business transactions and commercial business affairs. The word "Consumer" means any natural person. That could be an individual sole proprietor. It could be the personal guarantor who guarantees a business debt or it could be the owner of a small business who decides to pay for business goods with a personal credit card. The personal information which these laws intend to protect is generally defined as information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular Consumer. One often thinks of this kind of personal information as being a name, address, social security number, bank account number, cellphone or landline number; but in many states, it specifically includes biometrics.

Let's take a look at some of the recent legislation which has passed and is effective or is about to become effective in the near future.

California Consumer Privacy Act (CCPA"), which was enacted in 2018 and has been enforceable since January 2020 was amended by **The California Consumer Privacy Act (CCPA"). The California Privacy Rights Act ("CPRA")** was voted upon by the citizens of California in November 2020 as Proposition 24; and as expected, it passed. It is now law and becomes effective January, 2023. The CPRA amends the CCPA in many ways. What is favorable to some companies is that those companies who have already geared up to be compliant with GDPR will have already met a lot of the CPRA requirements. Among other things, the CPRA created a new state agency, the California Privacy Protection Agency, which will have rule-making and enforcement authority. While it brings the CCPA more in line with the GDPR, one favorable aspect is that businesses will not be held responsible for CPRA violations committed by third parties if certain agreements are in place and the business partner itself is in compliance with CPRA. The CPRA requires businesses to include specific provisions in their contracts with service provides, contractors, and third parties. Businesses must identify the "limited and specified" purposes for which the recipient of personal information processes that information, and they must prohibit service providers and contractors from combining the information they receive from the business with information from other entities.

Those entities which are compliant with the Gramm Leach Bliley Act **("GLB")** Safeguard Rule may be exempt from any further compliance requirements.

continued on next page...

In this Issue

Management Team

Congratulations to Sandra Rushing from Lineage Logistics PFS, LLC. on winning an Echo Show 5 in our drawing.

Make sure to enter this month's drawing by using your Special Placement form. For every claim you place you will be entered for a chance to win an Echo Show 5.

Certified By CLLA
Endorsed By IACC

con't

Virginia has become the second state, after California, to pass data privacy legislation. Known as the **Consumer Data Protection Act**, the law would go into effect January 1, 2023. This **CDPA** would apply to all businesses that control or process data for at least 100,000 Virginians, or those commercial entities that derive at least 50 percent of their revenues from the sale and processing of consumer data of at least 25,000 customers. The law would exempt health care data and information collected for assessing credit worthiness. Similar to the CCPA, consumers will have the right to know whether their data is being collected and processed. Consumers will be entitled to a copy of their data and may correct inaccuracies. Consumers will have the right to have their personal data deleted and may opt out of the processing of personal data that may be used for targeted advertising, sale, or consumer profiling.

Washington State has pending the **Washington Privacy Act ("WPA")** which contains many of the requirements of the CCPA and CDPA but also focuses on "controllers" and "processors" like the GDPR. One of three criteria must be met for the Washington Privacy Act to apply: 1) the legal entity conducts business in Washington or produces products or services that are targeted to residents of Washington and 2) during a calendar year, an entity must control or process data of 100,000 Washington residents/ consumers or more; 3) the legal entity must derive 25 percent of its gross revenue from the sale of personal data and processes or controls personal data of 25,000 consumers or more. The WPA generally excludes from its provisions the same information and entities as does the CCPA, including "personal data collected, processed, sold or disclosed pursuant to the **GLB…."** If signed into law, the **WPA** would be generally effective July 31, 2022 with respect to the processing of personal data.

Nevada very quietly passed its own tougher online privacy law in 2019. Although quiet by comparison to California's CCPA, it was the first state to amend its existing privacy law by requiring businesses to offer consumers an opt-out regarding the sale of their personal information, with some exceptions. The statute went into effect October 1, 2019. Unlike CCPA and GDPR, Nevada's bill does not add any new notice requirements for website operators but does require them to post certain items of information in their privacy policies, including the categories of information collected, the categories of third parties with which the data is shared, a description of the process consumers may use to review and request changes to their covered information, a disclosure that third parties may track consumers' online activities and the effective date of these notices.

Maine passed its Act to Protect the Privacy of Online Consumer Information which was signed into law by Governor Janet Mills on June 7, 2019. The Privacy statute became effective on July 1, 2020. The legislation specifically bars broadband internet access providers from "using, disclosing, selling or permitting access to customer personal information unless the customer expressly consents to that use, disclosure, sale or access," with some exceptions. The bill also prohibits broadband providers from refusing to serve a customer or charging them more if they don't consent to the use, disclosure, sale or access of their personal data. The bill further requires providers to take reasonable measures to protect customer personal information from unauthorized use, disclosure, sale or access.

This article is the author's update from her "Legislative Update" which was published in Vol. 53 Issue 1 of SCOPE, (a publication of the International Association of Commercial Collectors)