Published on *The National Law Review* https://natlawreview.com

Financial institution confusion: Are financial institutions fully exempt from the CCPA, CPRA, VCDPA, and CPA?

Article By:

David A. Zetoony

The Gramm–Leach–Bliley Act (GLBA) and its implementing regulations impose privacy requirements when financial institutions collect "nonpublic personal information about individuals who obtain financial products or services primarily for personal, family, or household purposes."[1] GLBA does not apply, however, when a financial institution collects information about individuals "who obtain financial products or services for business, commercial, or agricultural purposes" – such as information collected when providing commercial loans, commercial checking accounts, or other B2B services.[2] GLBA also does not apply when a financial institution collects information from an individual that is not applying for a financial product. For example, GLBA would not govern the collection by a financial institution of information from, or about, visitors to the institution's website who do not have (or are not seeking) a relationship with the institution;[3] nor would GLBA govern the collection by a financial institution of information from, or about, its employees. GLBA preempts state laws only to the extent that compliance with a state law would be "inconsistent with" the requirements of the GLBA.[4] A state law is not considered "inconsistent" if it provides a person with "protection" that "is greater than the protection provided" under the GLBA.[5] As a result, it is possible for state data privacy laws to apply to financial institutions so long as they do not purport to weaken privacy protections and the state law does not provide its own financial institution exemption.

Some state privacy laws, such as the CCPA, do not provide a blanket exemption for financial institutions, but instead contain a partial exemption for information collected by financial institutions where the information is itself subject to the GLBA (e.g., information about individuals who have obtained personal financial products from the institution). Such information is exempt from the privacy requirements of the CCPA, but, is not exempt from the private right of action conferred if a business fails to implement and maintain reasonable security to protect certain categories of information. The relatively narrow scope of the exemption contrasts with broader exemptions provided by other states. It is also worth noting that while other state privacy laws, such as Colorado's CPA may fully exempt financial institutions that are subject to GLBA, some of their substantive provisions overlap with other state laws that do not provide for such an exemption. For example, the CPA imposes an obligation that entities implement reasonable security to protect personal data. While that obligation does not apply to financial institutions a materially similar obligation is imposed within the Colorado safeguards statute.[6] Financial institutions are not fully exempt from the obligation imposed by the safeguards statute, however, that statute does deem a financial institution in compliance so long as the financial institution maintains procedures that comply with GLBA.[7] The net result is that if a financial institution

was found to have violated the data security requirements imposed by the GLBA by not maintaining data security related policies, procedures, or protocols sufficient to satisfy the GLBA, there would be a strong argument that the financial institution could not be found liable under the CPA (based upon the financial institution exemption found within that statute), but might be found liable under the Colorado safeguards statute.

The following chart compares the financial institution exemption provided by the main state data privacy laws:

Applicability of State Comprehensive Privacy laws to Financial Institutions Subject to GLBA

California (CCPA)	**California (CPRA effective 2023)**	**Nevada (Online Privacy Notice Statute)**	**Virginia (VCDPA)**	**Colorado (CPA)**
Text of exemption	Statute does not apply to "personal information collected, processed, sold, or disclosed pursuant to the federal Gramm-Leach-Bliley Act (Public Law 106-102), and implementing regulations . . . . This subdivision shall not apply to Section 1798.150 [of the CCPA].[8]	Statute does not apply to "personal information collected, processed, sold, or disclosed subject to the federal Gramm-Leach-Bliley Act (Public Law 106-102), and implementing regulations . . . . This subdivision shall not apply to Section 1798.150 [of the CCPA].[9]	Statute does not apply to a "financial institution or an affiliate of a financial institution that is subject to the provisions of the Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6801 et seq., and the regulations adopted pursuant thereto.[10]	Statute does not apply to "any . . . financial institution or data subject to Title V of the federal Gramm-Leach-Bliley Act (15 U.S.C. § 6801 et seq.) . . . ."[1] [1] Va. Code 59.1-572(B) (2021).
Personal Accounts (**Data Privacy** Obligations). Does state statute impose data privacy obligations upon personal data subject to GLBA (i.e., nonpublic information about consumer accounts)	**X**	**X**	**X**	**X**
Personal Accounts	[redacted]	[redacted]	N/A[14]	**X**

(**Data Security** Obligations). Does state statute impose data security obligations upon personal data subject to GLBA (i.e., nonpublic information about consumer accounts)				
Non-Personal Accounts (**Data Privacy** Obligations). Does state statute impose data privacy obligations upon data not subject to the GLBA, if the financial institution is itself subject to GLBA (e.g., nonpublic information about business accounts)			**X**	**X**
Non-Personal Accounts Exempt (**Data Security** Obligations). Exemption arguably covers data not subject to the GLBA, if the financial institution is itself subject to GLBA (e.g., nonpublic information about business accounts)			N/A[15]	**X**

[1] 12 C.F.R. 216.1(b). See Q 418 for a comparison of the substantive requirements of the GLBA with the substantive requirements of the CCPA, and the CCPA as amended by the CPRA.

[2] 12 C.F.R. 216.1(b).

[3] Federal Reserve, Regulation P: Privacy of Consumer Financial Information Frequently Asked Questions, at B.5 (Dec. 2001).

[4] 15 U.S.C. 6807(a).

[5] 15 U.S.C. 6807(b). Note, however, that some states have deferred to federal regulation of financial institutions by voluntarily exempting from the scope of their privacy statutes financial institutions that are subject to GLBA regulation.

[6] C.R.S. 6-1-713.5(1) (2021).

[7] C.R.S. 6-1-713.5(4) (2021).

[8] Cal. Civ. Code § 1798.145(e) (West 2020).

[9] Cal. Civ. Code § 1798.145(e) (West 2020).

[10] N.R.S. 603A.330(2)(b) (2021).

[11] Va. Code 59.1-572(B) (2021).

[12] C.R.S. 6-1-1304(2)(j)(II) (note that the statutory citation is based off SB 21-190 which still awaits governor approval).

[13] C.R.S. 6-1-1304(2)(q) (note that the statutory citation is based off SB 21-190 which still awaits governor approval).

[14] Note that while the Nevada Online Privacy Notice statute does not impart data security obligations, Nevada has other statutes which do impose obligations to secure personal information or to report data breaches. Financial institutions are not fully exempt from those provisions.

[15] Note that while the Nevada Online Privacy Notice statute does not impart data security obligations, Nevada has other statutes which do impose obligations to secure personal information or to report data breaches. Financial institutions are not fully exempt from those provisions.

National Law Review, Volume XI, Number 183