

Data Security and Privacy

Protecting Consumers and Ensuring Effective Security Practices



ACA International, the Association of Credit and Collection Professionals, supports state data security legislation that protects consumers without imposing unreasonable burdens and barriers on the credit and collection industry. While ACA recognizes the important role data security legislation plays in protecting personal consumer information and ensuring consumer notice in the event of a security breach, well-intentioned legislative efforts should not create unnecessary and unintended liability or burdens for the credit and collection industry.

Background

Debt collectors rely on sensitive personal information to properly identify a consumer and establish the accuracy of the debt. While consumer sensitive information may be used for other purposes, such as to evaluate a consumer's ability to pay a past due account, the credit and collection industry appreciates the sensitive nature of personal information and is committed to keeping such information secure and private.

The credit and collection industry has a strong economic incentive to assure personal consumer information is secure and private. The failure to maintain data privacy and security increases the potential for identity theft, which can result in significant economic harm to debt collectors and their creditor clients. Protection of personal consumer information is a sound and widely adopted business practice by members of the credit and collection industry.

Uniform application to public and private sectors

ACA believes state data security legislation should apply uniformly to private businesses and government entities alike given that governments, government subdivisions, and government agencies and instrumentalities retain a significant amount of personal information.

Overlapping laws

The collection industry is strictly regulated through existing and overlapping federal legislation, including the Fair Debt Collection Practices Act (FDCPA), the Fair Credit Reporting Act (FCRA), the Gramm-Leach-Bliley Act (GLBA), and the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Debt collectors are also subject to a myriad of state laws and regulations and state common law. These regulations already require data security and privacy of personal consumer information.

To prevent overlapping and potential inconsistencies with federal security and privacy mandates, ACA believes state data security laws and legislation should provide that debt collectors in compliance with either the GLBA or HIPAA are deemed compliant with any state-imposed security, privacy and notification requirements.

Inconsistent laws

ACA believes state data security and privacy laws and legislation, which may require notice be sent to consumers, should expressly state that such notices are not communications as defined by the Fair Debt Collection Practices Act (FDCPA) or the state's own fair debt collection practices act.

Under the FDCPA, a debt collector may be prohibited from providing notices to consumers that are mandated by state data security or privacy laws upon receiving a consumer's request to cease communication or refusal to pay the debt. This leaves debt collectors faced with violating federal law by providing such notification or violating applicable state law for failing to provide the required notification. Expressly including such notices from the definition of a communication protects consumers and maintains clarity for businesses providing the notices.

ACA International, the Association of Credit and Collection Professionals, is the primary trade association for members of the credit and collection industry and has been a leading source for industry information and education for more than 65 years. The association has more than 5,500 members, including third-party debt collectors, asset buyers, attorneys, credit grantors and vendor affiliates.