AFSA
AMERICAN FINANCIAL SERVICES ASSOCIATION

DATA BREACH LEGISLATION

In November 2013, newspapers reported that Target stores had been attacked by hackers who had stolen payment data including names, addresses and phone numbers from around 40 million credit and debit cards, leaving the retailer's customers open to fraud and identity theft. This was followed in 2014 by Staples' announcement that 1.16 million cards had been compromised in a data breach, and shortly after that, by Home Depot's announcement that a staggering 56 million consumers had been exposed by hackers accessing their systems.

These high-profile events raised public awareness about the dangers of data breaches, which continue to occur on a daily basis. According to the Identity Theft Resource Center (ITRC), the number of significant U.S. data breaches in 2015 totaled 781, the second highest year on record since the ITRC began tracking breaches in 2005.

These data breaches have compelled policymakers to act at the state and federal level. Legislation has been introduced that seeks to mandate the notification that breached parties must give to affected consumers. A number of states have looked to introduce laws of their own alongside new federal laws.

ISSUE BRIEF

AFSA'S POSITION

AFSA believes that in order to provide meaningful and consistent protection for all consumers, all entities that handle sensitive consumer information should be subject to a uniform national notification standard.

At least thirty states have enacted security breach notification laws that impose conflicting or inconsistent requirements on business. For example, a statute in Illinois prevents delaying notification where requested by law enforcement (for the purposes of investigation), while other states require such a delay. These statutes differ widely in the information that they protect, the circumstances under which a notice to consumers is required, the third parties who must be notified in the event of breach, and the required content of the consumer notice.

The net effect is inconsistent state laws which result in higher compliance costs, uneven consumer protection, challenges for law enforcement, and confusion.