Banking and Finance Law Daily Wrap Up, CREDIT, DEBIT AND GIFT CARDS—Data security 'long overdue,' say industry groups, urge Congressional cosponsorship, (Oct. 16, 2015)

Click to open document in a browser

By Colleen M. Svelnis, J.D.

A consortium of trade associations has signed a joint letter to Congress in support of H.R. 2205, the Data Security Act of 2015, and urging Representatives to cosponsor the bill. The letter, from trade groups including the Consumer Bankers Association, American Bankers Association, and Independent Community Bankers of America, states that "data security requires all participants in the payments ecosystem–financial institutions, payment networks and processors, and merchants–to do their part to ensure that consumers' sensitive payment information is protected. The payments system is only as strong as its weakest link; that is why we urge you to cosponsor H.R. 2205." The letter noted that the cost of reissuing payments cards disproportionally falls on small financial institutions and said it is "long overdue" for Congress to pass legislation addressing data security.

Retailers are not subject to data security requirements similar to those financial institutions of all sizes are subject to under the Gramm-Leach-Bliley (GLB) Act, but as the letter states "recent history shows that it is clearly vital to protect data on both sides of the transaction." H.R. 2205 would ensure "that all entities that handle consumers' sensitive financial data have in place robust processes to protect data which should help prevent data breaches in the first place," says the group.

Background. The Data Security Act of 2015, H.R. 2205, a bipartisan bill that would establish a national data security and breach notification standard for all businesses, was introduced by Reps. Randy Neugebauer (R-Texas), Chairman of the Financial Institutions and Consumer Credit Subcommittee, and John Carney (D-Del), a member of the Financial Services Committee. The Data Security Act would apply to any individual, partnership, corporation, trust, estate, cooperative, association, or entity that accesses, maintains, communicates, or handles sensitive account information or sensitive personal information (see *Banking and Finance Law Daily*, May 4, 2015).

The bill directs covered entities to develop an information security plan that requires them to:

- designate at least one employee to manage safeguards;
- conduct risk analyses;
- regularly assess the plan in light of risks; and
- update the program on a rolling basis as technology evolves.

Under the bill, if a covered entity believes that a data breach has or may have occurred involving sensitive financial account information or sensitive personal information, the company must conduct an investigation. The trigger for notification occurs only after a company confirms that the unauthorized acquisition of the information is reasonably likely to cause substantial harm to the consumers to whom the information relates, the covered entity, or a third party acting on behalf of the entity.

Call to action. The industry associations call data security a "shared responsibility" by all participants, and "strongly urge" the representatives to cosponsor H.R. 2205, "which will help ensure that minimum standards are in place to protect your constituents' sensitive financial and personal information."

Companies: American Bankers Association; Consumer Bankers Association; Credit Union National Association; Electronic Payments Coalition; Financial Services Roundtable; Independent Community Bankers of America; National Association of Federal Credit Unions

IndustryNews: ConsumerCredit CreditDebitGiftCards IdentityTheft Privacy

©2015 CCH Incorporated and its affiliates and licensors. All rights reserved.
Subject to Terms & Conditions: http://researchhelp.cch.com/License_Agreement.htm