



Legislative & Regulatory Update

3rd Quarter 2011

Electronic Transactions Association
1101 16th Street NW, Suite 402
Washington, DC 20036
202.828.2635 www.electran.org

SUMMARY

Federal and state legislative activity slowed this quarter due to summer recess in many chambers. Federal activity continued on data security and 6050W merchant reporting.

Advocacy efforts in the data security debate continued as the focus of activity moved to the Senate in September. ETA's delivered a letter to the Senate Judiciary Committee outlining

Support for various aspects of three data security bills, as well as the association's concerns about other provisions in the measures. Congressional consideration of data security legislation will continue in 2012, and these three bills will carry over into the next session of Congress.

In early October, ETA alerted members to a late-arriving revision of Form 1099K, accompanied by proprietary IRS merchant category codes (MCCs), which has an impact on 6050W merchant transaction reporting. The revised form called for the reporting of information not previously requested by the IRS, causing hardship for many ETA members. ETA drafted a letter to the IRS outlining the difficulties of this new, unanticipated requirement and asked for a one year delay in implementation of it.

FEDERAL LEGISLATION AND REGULATION

Consumer Financial Protection Bureau

Congress

2011-10-06: *Senate Banking Committee approves CFPB nominee*

The committee voted to send the nomination of Richard Cordray as head of the new Consumer Financial Protection Bureau to the full Senate. Republicans have promised to block the Senate from voting on Cordray until changes are made to the structure of the bureau.

Executive

2011-10-03: *President Obama says bank fees are reason for CFPB*

President Barack Obama pointed to Bank of America's decision to charge some of its customers a \$5 monthly fee for debit-card purchases as an example of why the U.S. needs a strong consumer watchdog. Mr. Obama said the debit-purchase fees are "exactly why we need somebody whose sole job it is to prevent this kind of stuff from happening." Mr. Obama suggested the federal government could crack down on fees when banks are treating consumers unfairly. "You can stop it," he said, adding that the government can tell the banks "you don't have some inherent right just to, you know, get a certain amount of profit, if your customers are being mistreated."

Data Security / Breach Notification

Congress

2011-09-22: *Senate Judiciary passes data security bills*

The committee passed an amended version of S. 1151, the "Personal Data Privacy and Security Act of 2011". This bill would require firms to safeguard sensitive information, such as Social Security and credit card numbers, and to notify consumers in the event of a security breach. In

Electronic Transactions Association Board of Directors Meeting

the event of a breach, notification would be required to any resident of the US whose personal information “has been, or is reasonably believed to have been, accessed, or acquired,” unless a risk assessment shows there is “no significant risk of harm” to consumers. The bill would also impose criminal penalties on individuals who intentionally and willfully conceal the fact that a data breach has occurred. The committee also passed amended versions of S.1408, the “Data Breach Notification Act of 2011” and S.1535, the “Personal Data Protection and Breach Accountability Act of 2011”.

ETA Action: ETA submitted a letter to the Senate Judiciary Committee outlining areas of agreement and concern with each of the three bills.

2011-08: *Senate establishes working groups for data security legislation coordination*

Senate Majority Leader Harry Reid proposed working groups to be made up of staff from different Senate committees to negotiate an agreement with the Obama administration on legislation that can proceed directly to the floor. The White House’s proposal must be reconciled with various cyber security bills that have been crafted in the Senate, including a measure (S. 773) introduced in the previous Congress by Senate Commerce, Science, and Transportation Chairman Jay Rockefeller (D-WV.) and similar legislation (S. 413) that has been reintroduced by Senate Homeland Security and Governmental Affairs Chairman Joseph Lieberman (I-CT).

2011-07-28: *S.1434, the “Data Security Act of 2011,” introduced by Sens. Thomas Carper (D-DE) and Roy Blunt (R-MO)*

This bill, introduced by Sen. Carper (D-DE) for the fourth time, would require businesses and federal agencies to adopt data security measures to protect personal information—primarily financial data—and mandate notification to individuals of breaches of their personal data. The bill, which is modeled on data security provisions of the Gramm-Leach-Bliley Act and its implementing regulations, would preempt state data security and breach notification laws.

S. 1434 would require businesses that handle sensitive consumer data, electronic or paper, to implement information security safeguards, investigate security breaches, and notify consumers if their “sensitive account information” or “sensitive personal information” in a readable or usable form is breached. The bill does not require breach notice of covered information if it is “maintained or communicated in a manner that is not usable (I) to commit identity theft; or (II) to make fraudulent transactions on financial accounts.” Data that is maintained or sent in “encrypted, redacted, altered, edited, or coded form” is considered unusable.

Federal Communications Commission

Executive

2011-09-23: *FCC publishes net neutrality rules*

The FCC’s “Open Internet” order and rules were published in the Federal Register, nine months after adoption, and will officially take effect Nov. 20. The rules aim to prevent internet service providers from blocking access to certain web sites or applications, but have been mired in controversy since the agency voted to enact them on a partisan, 3-2 vote last December.

Financial Stability Oversight Council

Executive

2011-10-06: *Treasury Secretary Geithner announces new guidance*

The secretary said a new council of government regulators (FSOC) will issue guidance in the next week that will illustrate how they will designate nonbank financial firms as systemically important financial institutions (SIFIs). Insurance firms, hedge funds, money market funds, and other financial enterprises could be designated as SIFIs and made subject to bank-like supervision by the Federal Reserve.

Internal Revenue Service

2011-09: *IRS releases new version of Form 1099K for 6050W merchant reporting*

The IRS revised, for a third time, Form 1099K that merchant acquirers must use when reporting merchant card transactions to the IRS, beginning in January 2012. The new form includes a box for each merchant's category code (MCC). The IRS provided a list of MCCs in their original release of the new form; the IRS has since removed this list from circulation.

ETA Action: On October 3, ETA sent a Regulatory Alert to all members through The Voice of Payments™ web portal to inform them of this new 1099K reporting development. On October 5, Digital Transactions published an article, "Yet Another New IRS Tax-Reporting Revision Adds to Acquirers' Burdens," which quoted ETA staff expressing concern over the addition of a new data reporting requirement nine months into the reporting year and the fact that the IRS MCC list did not exactly match current MCCs utilized in the payments industry. On October 13, ETA was informed by the IRS that they had removed their MCC list from circulation and that they will accept current MCC codes in 1099K reporting. In addition, the Government Relations committee is preparing a letter to the IRS calling attention to the difficulties of implementation and requesting a one-year delay in implementation of the MCC requirement.

STATE LEGISLATION AND REGULATION

California

2011-08-31: *Gov. Brown signs new breach notification law (S.B. 24)*

As of Jan. 1, 2012, California businesses and agencies that are required to provide notice to individuals of the breach of their personal data also must notify the state Office of the Attorney General of an information breach of more than 500 California residents. The new law requires, for the first time, that notices to individuals include certain information such as: the type of information breached, the time of the breach, and a toll-free telephone number of major credit reporting agencies. The law also amends the substitute notice provisions for breaches that require notice to more than 500,000 state residents or cost more than \$250,000 to send individual notices. In addition to placing substitute notice of a breach on their websites and in major statewide media, business will have to notify the California Office of Privacy Protection.

Electronic Transactions Association Board of Directors Meeting

New York

2011-09-29: *Tax Department bulletin clarifies sales tax on customer loyalty cards*

The New York State Department of Taxation and Finance issued a tax bulletin (TB-ST-145) to clarify how sales taxes apply to purchases involving customer loyalty cards and what steps retailers must take to ensure proper recordkeeping, reporting, and payments.

Texas

2011-06-17: *Gov. Perry signs breach law intended to cover entire country*

Texas expanded the scope of its information security breach notification law to protect residents of all 50 states. To date, 46 states plus the District of Columbia, the U.S. Virgin Islands and Puerto Rico have enacted laws requiring businesses to notify individuals when there has been a breach of their sensitive personal information. Texas's law was amended to cover the remaining four states, Alabama, Kentucky, New Mexico and South Dakota. The new law applies not only to residents of Texas but to any individual whose sensitive personal information was, or is reasonably believed to have been, acquired by an unauthorized person, regardless of their state of residence.

Texas's law specifically requires notification of data breaches to residents of states that have not enacted their own law requiring such notification. This amendment purports to add an obligation to notify individuals who would otherwise not be required to be notified under any law, and provides for penalties (which would be paid to Texas) if such non-Texas residents are not notified of an information security breach suffered by an entity that "conducts business in" Texas.

In addition, Texas's new law also requires notification to residents of every state outside Texas that does have its own breach notification law in place—however, notification under the roughly 46 existing state laws is deemed to constitute compliance with the Texas law. Although this might at first blush seem not to add any exposure that did not already exist, the heightened penalties under the Texas law effectively increase the liability exposure for any entity conducting business in Texas if that entity suffers a data breach and fails to notify any non-Texas residents of the breach.