CHAPMAN AND CUTLER LLP

To the Point!

legal, operations, and strategy briefs for financial institutions February 20, 2014

Making a Virtual Bank ADA Compliant

We published an article in the February 2014 edition of *The Banking Law Journal* exploring access to private websites for individuals with disabilities. The article discusses circumstances in which the Americans with Disabilities Act ("ADA") has been applied to private websites, including regulatory enforcement and litigation and the current Department of Justice ("DOJ") initiative to establish technical guidelines for ADA website compliance. Based on the Advance Notice of Proposed Rulemaking it is anticipated that the DOJ will adopt rules to ensure ADA compliance of private websites perhaps similar to the rules that now apply to automated teller machines. We encourage banks to become familiar with and monitor the progress of the DOJ's rulemaking. You can access our article here. The DOJ anticipates a release of a Notice of Proposed Rulemaking toward the middle of the government's fiscal year 2014.

Incident Response Plan for Privacy and Data Security Breaches

Even if your institution has not experienced an internal breach of data security, the massive data breaches at Target and Neiman Marcus in December 2013 may have directly affected your financial institution or your customers. In fact, financial institutions have reported an estimated card replacement cost of $200 million alone and no estimates of fraudulent transactions, credit monitoring or other costs have been released.

We recommend that your institution adopt a formal incident response plan to address data security breaches. An incident response plan should be tailored to the institution and its data security risks, and address both internal and external data breach incidents that affect its customers, such as the Target and Nieman Marcus breaches.

Such a plan should identify an incident response team comprised of members from key groups, such as information technology, privacy office, compliance, legal, customer service, business managers, and public relations. The plan should outline steps to be implemented when the incident response team receives a notice of a potential data breach. The steps may include: initial assessment and investigation of the suspected breach, initial response to mitigate the impact of the incident, notification of regulators, customers, and third parties such as vendors, and implementation of changes to prevent future incidents. The plan should include both internal and third party resources needed to implement actions directed by the team, such as call center coverage, mail resources, credit monitoring services, and crisis management personnel.

An incident response plan can facilitate the decision-making process in response to a data breach and save valuable time in executing a response. Having such an incident response plan in place demonstrates that the institution takes its customers' privacy and security seriously.

Telephone Consumer Protection Act ("TCPA") Update

As previously reported in our May 16, 2013 *To the Point*, an individual can bring an action under the TCPA and collect $500 or actual damages, whichever is greater, in the event of an alleged violation. Treble damages are available for a willful or knowing violation, making class action lawsuits attractive. We provided further update in our August 29, 2013 *To the Point* on amendments to the Federal Communications Commissions rules and cases.

The TCPA provides that cell phones can only be called using an automatic dialer if the customer has provided express consent and cell phones can only be called for telemarketing purposes with prior written consent. Finally, courts have determined that text messages and email messages converted to text messages are "calls" subject to the TCPA limitations.

Litigation continues to grow and in 2013 banks entered into large settlements related to contact with customers on cell phones. We urge businesses to update their agreements with customers to address the variety of ways in which a business may communicate with its customers and to secure the express consent, including an right to opt-out, that will allow communication to continue without risk of liability under the TCPA.

FinCEN Issues New Guidance on Virtual Currencies

On January 30, 2014, the Financial Crimes Enforcement Network ("FinCEN") published two administrative rulings, providing guidance to supplement its initial guidance from March 2013 on whether a party engaging in certain activities involving convertible virtual currency meet the definition of a "money transmitter" subject to the Bank Secrecy Act ("BSA").

The March 2013 guidance from FinCEN described three types of participants in the virtual currency markets:

- An "administrator" issues virtual currency and has the authority to redeem (to withdraw from circulation) the virtual currency.
- An "exchanger" is engaged in the business of exchanging virtual currency for traditional currency or another virtual currency.
- A "user" obtains virtual currency and uses it to purchase goods or services.

Under the above guidance, "administrators" and "exchangers" are "money transmitters" subject to the BSA that must register and comply with regulations applicable to a money services business ("MSB"), and "users" are not.

Through its recent administrative rulings, FinCEN clarified which entities are users, not subject to the BSA, by stating that: (1) an entity that "mines" convertible virtual currency for personal purposes is not a money transmitter; and (2) a software company that purchases, and sells convertible virtual currency for its investment purposes, and produces and distributes software to facilitate the purchase is a user. Together, these rulings clarify that obtaining virtual currency for personal use and exchanging it for traditional currency for personal use would not trigger MSB status.

Virtual currency administrators and exchanges operating as MSBs will continue to face challenges in terms of complying with FinCEN regulations and state-level money transmitter licensing and regulatory requirements. Virtual currency has been in the news recently due to the high profile case involving usage of such currency on the Silk Road website as a means of money laundering, for drug trafficking and other criminal activities. Virtual currency is a growing area but its usage generally has not drawn scrutiny from regulators in the United States. However, if usage of virtual currency continues to grow in acceptance, we anticipate more guidance to come from other financial system regulators.

Chapman and Cutler LLP

Attorneys at Law · Focused on Finance®

To the Point! is a summary of items of interest and current issues for financial institutions with primary focus on regulatory, consumer, and corporate issues. Chapman and Cutler LLP maintains a dedicated practice group with expertise to counsel on these issues and other enterprise risk management matters facing financial institutions. If you would like to discuss any of the items contained in these briefings or other legal, regulatory, or compliance issues facing your institution, please contact one of the partners in our Bank Regulatory Group:

Marc Franson • 312.845.2988
Scott Fryzel • 312.845.3784
Heather Hansche • 312.845.3714
Doug Hoffman • 312.845.3794
John Martin • 312.845.3474
Dianne Rist • 312.845.3404

Chapman and Cutler LLP | 312.845.3000 | 111 West Monroe Street | Chicago | IL | 60603