Chapman and Cutler LLP

To the Point!

February 19, 2016 Legal, Operations and Strategy Briefs for Financial Institutions

Standards for Safeguarding Customer Financial Information

The Federal Trade Commission (*"FTC"*) stated in a recent Federal Register Notice that it plans to review its existing Safeguards Rule for non-bank financial institutions under its jurisdiction. The FTC's Safeguards Rule applies to a broad range of non-bank companies, including finance companies and other non-bank lenders, check cashers, servicers, debt collectors, auto dealers, investment advisors, and consumer reporting agencies. The Safeguards Rule was established in 2002 under the Gramm-Leach-Bliley Act.

Since then, the FTC has brought over 50 enforcement actions for failure to take reasonable steps to protect consumers' financial information, using its authority under the Safeguards Rule and Section 5 of the FTC Act (*"UDAP"*). These enforcement actions have included actions against Wyndham Hotels, Twitter, Fandango, and Dave & Buster's.

The FTC has assumed a leading role in privacy and data security and has used its UDAP authority to bring enforcement actions establishing standards for acceptable conduct related to safeguarding consumer financial information. Generally, the FTC reviews its rules every ten years; the Safeguards Rule has been on the agency's agenda and then postponed twice, making it more likely that the review will occur this year. While the FTC's Safeguards Rule is not applicable to banks, we recommend that both banks and non-bank financial institutions monitor the FTC's review of safeguarding requirements and consider how its proposals, if adopted, will affect what is deemed to be a "reasonable" safeguarding practice.

HIPAA Data Breach Notification Deadline—February 29, 2016

Covered entities that experienced data breaches of unsecured protected health information affecting fewer than 500 individuals during 2015 have until February 29, 2016, to file their required notice(s) with the U.S. Department of Health and Human Services (*"HHS"*), Office for Civil Rights.

Although HIPAA does not require the business associates of covered entities to provide this HHS notice, business associates, including banks, should review their Business Associate Agreements (*"BAA"*) with covered entities and identify their contractual requirements related to these data breaches. For example, the terms of a BAA may require the business associate to provide the covered entity with notice of each data breach (generally within 60 or fewer days of the breach), maintain records of the data breach, provide the covered entity with sufficient information and assistance to enable it to complete its notification requirements, and require the business associate to take remedial action. The BAA could also require the business associate to make the data breach filing on behalf of the covered entity.

Since there is no single required form of BAA that covered entities must use, each BAA may be a custom, negotiated agreement and each business associate should take steps to ensure that it has procedures in place to enable it to comply with both the statutory requirements applicable to it and the contractual requirements for each of its covered entities.

CFPB Issues Additional Guidance on Furnisher Obligations under Regulation V

The CFPB continues to focus on furnishers of information to consumer reporting agencies (*"CRAs"*). In September 2013, the CFPB issued a bulletin identifying furnishers' obligations under Regulation V to furnish information that is accurate and complete and to investigate consumer disputes about the accuracy of information they provide.

Based on its subsequent supervisory experience, the CFPB issued another bulletin on furnisher obligations in February 2016, this time emphasizing that furnishers are obligated to have reasonable written procedures regarding accuracy of consumer information furnished to all CRAs—not just to nationwide CRAs (*i.e.,* Experian, Equifax, and TransUnion), but also to specialty CRAs such as those that obtain deposit account information.

The CFPB specifically identified compliance failures of furnishers with respect to specialty CRAs and stated in the bulletin that it will continue to monitor furnishers' compliance with this aspect of Regulation V. Failure to comply may result in supervisory and enforcement actions, and the CFPB may assess remedial measures, including redress to consumers.

Financial institutions should determine whether they report information to specialty CRAs. If so, they should review their compliance policies and procedures to ensure they are reasonable and satisfy the Regulation V requirements for furnishing information to both nationwide and specialty CRAs. In particular, the policies and procedures should take into consideration the differences in furnishing information to nationwide and to specialty CRAs, including the type, frequency, and nature of information supplied.

Court Denies Motion to Dismiss Complaint Against MoneyGram Chief Compliance Officer for Bank Secrecy Act Violations

In 2012, MoneyGram entered into a deferred prosecution agreement with the U.S. Department of Justice and the U.S. Attorney's Office for the Middle District of Pennsylvania on charges of aiding and abetting wire fraud and willfully failing to implement an effective anti-money laundering (*"AML"*) program. In its lawsuit filed in December 2014, FinCEN sought to collect a $1 million dollar fine from MoneyGram's Chief Compliance Officer and bar him from service to any U.S. financial institution.

The defendant filed a motion to dismiss on multiple grounds, including that an individual officer of a financial institution cannot be held personally liable for the entity's failure to implement an effective AML program under the Bank Secrecy Act. The U.S. District Court disagreed and in its January 8, 2016, ruling stated that civil penalties may be imposed on corporate officers and employees responsible for designing and implementing an entity's AML program if it is determined that the entity failed to implement an effective AML program. Financial institution officers and employees responsible for AML compliance now face new personal risks and should to continue to watch this case closely.

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 maintains a dedicated practice group with the experience 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 members of our Bank Regulatory Group:

Marc Franson • 312.845.2988
Heather Hansche • 312.845.3714
John Martin • 312.845.3474
Scott Fryzel • 312.845.3784
Dianne Rist • 312.845.3404
Lindsay Henry • 312.845.3869