CHAPMAN AND CUTLER LLP

To the Point!

legal, operations, and strategy briefs for financial institutions February 12, 2013

Important Changes for Business Associates to the Privacy, Security, Breach Notification and Enforcement Rules Implementing Health Insurance Portability and Accountability Act ("HIPPA")

The Department of Health and Human Services ("HHS") issued its final rule implementing the Health Information Technology for Economic and Clinical Health Act ("HITECH Act") changes to the Privacy, Security, Breach Notification and Enforcement Rules governing protected health information ("PHI") under HIPAA (the "Rule"). The Rule is effective on March 26, 2013 and compliance is generally required by September 23, 2013. The following changes are important for financial institutions that are business associates.

When a Financial Institution is a Business Associate

A business associate is a company that has a covered entity (health care provider, health plan or health care clearinghouse) as a customer and receives, maintains or transmits PHI. A financial institution is not a business associate if its activities are limited to authorizing, processing, clearing, settling, billing, transferring, reconciling and collecting payments for health care or health plan premiums. Cashing a check or conducting a funds transfer are also activities that would not cause a financial institution to be deemed a business associate. However, a financial institution that receives, maintains or transmits PHI is a business associate when it performs functions "above and beyond the payment processing activities" such as accounts receivable functions.

Direct Compliance Responsibility for Business Associates

Business associates are now directly responsible for compliance with the HIPAA Security Rule and are subject to enforcement by HHS and state attorneys general. Each business associate will need to review the HIPAA Security Rule and revise its policies and procedures and institute employee training to ensure compliance with these requirements.

Business Associate Agreements

Each covered entity will need to enter into a new Business Associate Agreement ("BAA") with its business associates or amend its existing BAA to conform to these new requirements. As a result, business associates should be prepared to negotiate BAAs with each of their covered entities. HHS has published on its website sample provisions to be included in BAAs between covered entities and their business associates but does not provide a model form. Business associates and covered entities will be required to draft and negotiate their BAAs to include contractual rights and obligations and to satisfy the requirements of the Rule. The Rule contains extended compliance dates for changes to BAAs.

Business Associate and Its Subcontractors

The Rule expanded the definition of business associate to include all subcontractors of a business associate that perform functions for a business associate and require access to PHI. To illustrate, HHS provided in its notice issuing the Rule that a waste disposal company hired by a business associate to dispose of documents that include PHI would be considered a business associate.

Business associates are permitted to disclose PHI to subcontractors, provided the business associate obtains satisfactory written assurances from the subcontractor that the subcontractor will appropriately safeguard PHI. To ensure compliance with this requirement, each business associate will need to identify all subcontractors with access to PHI and review and amend, as appropriate, its agreements with these subcontractors to require compliance with the HIPAA Privacy, Security and Breach Notification Rules.

Breach Notification

The Rule also lowered the threshold for when a breach of unsecured PHI will require a breach notification. The former “risk of harm standard” required a determination that an incident poses a significant risk of financial, reputational or other harm to the individual before a breach notification was required. Now, if there is an impermissible use or disclosure of unsecured PHI, it is presumed to be a breach subject to the notification requirements unless the covered entity or business associate, as applicable, demonstrates based on a risk assessment that there is a low probability that the PHI has been compromised. This risk assessment must contain a review of the following four factors: (i) the nature and extent of the PHI involved, including types of identifiers and likelihood of re-identification; (ii) the unauthorized person who used the PHI or to whom the disclosure was made; (iii) whether the PHI was actually acquired or viewed; and (iv) the extent to which the risk to the PHI has been mitigated. Each business associate will be required to review and revise its policies and procedures to include this new analysis of a breach subject to the notification requirements and train its employees to follow the new procedures.

Civil Money Penalties

The Rule includes a scale of civil money penalties of $100 to $50,000 for each violation (with the highest penalties for willful violations), with a maximum for all identical violations of $1.5 million per year.

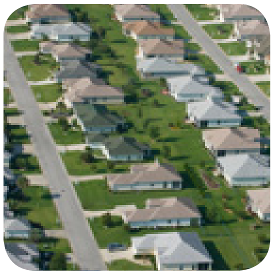
CFPB Seeks Information on Financial Products Marketed to Students

Congress included provisions in the CARD Act of 2009 to address problems it identified in the links between financial institutions and colleges, and marketing of credit cards to consumers under 21. The CARD Act restricted how card products can be offered to these consumers, required disclosures by financial institutions of their preferred lender arrangements with colleges and recommended that colleges adopt policies to limit campus marketing and establish debt education and counseling programs for students.

The CFPB has shown interest in the private student loans industry through its past requests for information on the industry and issuance of its report on issues facing private student loan borrowers. With the most recent Notice and Request for Information issued on January 31, 2013, the CFPB continues to scrutinize the links between financial institutions and colleges, seeking information on financial products and services marketed to college students and their experiences using these products and services. The CFPB has specifically included non-credit card financial products and services (i.e., checking accounts and debit card products) in this inquiry.

The CFPB’s request focuses on partnerships between colleges and financial institutions including campus affinity programs and specifically requests information on types of products tailored towards students, how these products are marketed, factors and information considered in choosing a product, types of fees charged, how much students pay in fees, how many students opt in for overdraft, and the students’ relationship with the financial institution after college. The CFPB also asks for comment on how these programs can be structured to promote positive financial decision-making and build money management skills for young consumers.

Financial institutions should identify, as applicable, their college affinity programs, products customized for college students and any marketing of standard products targeted to college students and consider responding to this request for information as the information the CFPB receives will likely form the basis for future rulemaking. Comments to the CFPB must be received by March 18, 2013.



In re Crane: An Update

As readers may recall, despite the "may be substantially in the following form" language in 765 ILCS 5/11, an Illinois Bankruptcy Court ruled that the elements enumerated in the statute were not permissive, but were required in order for a mortgage to provide constructive notice to a bona fide purchaser or a trustee in bankruptcy (In re Crane, U.S.B.C., C.D. Il., February 29, 2012). In response to this decision, the Illinois legislature passed an amendment to clarify that the requirements set forth in 765 ILCS 5/11 are permissive and not mandatory. The Governor signed the amendment into law on February 8, 2013. The Amendment becomes effective on June 1, 2013. Since the In re Crane decision, another Illinois Bankruptcy Court disagreed with the holding and concluded that use of the word "may" in 765 ILCS 5/11 clearly indicates that the provisions therein are permissive and not mandatory under the basic rules of statutory construction (In re Klasi Properties, 2013 WL 211111, U.S.B.C., S.D. Il., January 18, 2013). Until June 1, 2013 when the amendment becomes effective, we continue to suggest that Illinois mortgage lenders fully comply with 765 ILCS 5/11, including the use of an interest rate rider and inclusion of an express maturity date in mortgages and mortgage amendments.

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
David Worsley • 312.845.3896
Dianne Rist • 312.845.3404