

Alert 10-168



## Consumer Privacy Issues Abound in the Dodd-Frank Wall Street Reform and Consumer Protection Act

### *Bill Proposes a New Consumer Financial Services Agency with Considerable Privacy Responsibilities*

#### Introduction

With President Obama scheduled to sign the Dodd-Frank Wall Street Reform and Consumer Protection Act this week, the financial services industry faces a rapidly changing regulatory environment. While a great deal of attention has been paid to the significant restructuring of the financial services regulatory regime, little focus has been placed on the proposed changes to the oversight of consumer privacy issues, data security and data stewardship. These issues may not only affect banks, but all types of businesses servicing the financial industry as well.

#### The New Consumer Financial Protection Bureau ("CFPB")

Most noteworthy, in the privacy and data security context, is the establishment of the new CFPB, to be led by an independent director appointed by the president and confirmed by the Senate.<sup>1</sup> The new financial regulatory reform bill, known as the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank), creates a new consumer financial protection watchdog that comes armed with significant powers and rulemaking authority. Elizabeth Warren, Chair of the Nonpartisan Congressional Oversight Panel, a consumer advocacy organization, said, "They created a strong, independent consumer agency that will have the tools to rein in industry tricks and traps and to cut out the fine print. For the first time, there will be a financial regulator in Washington watching out for families instead of banks."<sup>2</sup>

#### CFPB Examination & Enforcement Authority

The CFPB will have authority to examine and enforce regulations for banks and credit unions with assets in excess of \$10 billion. CFPB will also govern mortgage-related businesses (lenders, servicers, mortgage brokers, and foreclosure operators), payday lenders, and student lenders, as well as other larger, non-bank financial companies, such as debt collectors and consumer reporting agencies, as will be determined by the CFBP in its regulations. Companies should closely evaluate Dodd-Frank and any implementing regulations adopted by the CFPB to determine whether and to what extent they are governed.<sup>3</sup> Companies that operate in a "grey area" of the proposed CFPB authority should consider whether advocacy during the implementing regulation rulemaking process would be advisable.

The CFPB has significant reach generally over businesses that provide "financial products or services," including service providers.<sup>4</sup> It will consolidate and strengthen consumer protection responsibilities currently handled by the Office of the Comptroller of the Currency, Office of Thrift Supervision, Federal Deposit Insurance Corporation, Federal Reserve Board, National Credit Union Administration, Department of Housing and Urban Development, and, to a lesser extent, Federal Trade Commission.

#### CFPB Rulemaking Authority

This new agency will be able autonomously to write rules for consumer protections governing many, if not most, businesses offering consumer financial services or products. The CFPB "may prescribe rules identifying as unlawful

unfair, deceptive, or abusive acts or practices in connection with any transaction with a consumer for a consumer financial product or service, or the offering of a consumer financial product or service."<sup>5</sup> Rules prescribed by the CFPB may include requirements for the purpose of preventing such unfair, deceptive, or abusive acts or practices.<sup>6</sup> The "unfair and deceptive" standard has been used by regulators in the privacy context before. For example, the Federal Trade Commission has used this authority to file actions against companies who have suffered a security breach, and companies whose privacy policies and information security practices were deemed inadequate.<sup>7</sup> With the added and undeveloped "abusive acts or practices" standard, the CFPB will have even broader authority to focus on privacy, data access rights, usage, disclosures, and information security issues.

While discussions are still ongoing, it appears that the CFPB will have rulemaking authority over specific enumerated laws pertaining to privacy issues, such as the Fair Credit Reporting Act and Gramm-Leach-Bliley, as well as laws that have been amended to permit CFPB jurisdiction, such as the Right to Financial Privacy Act of 1978 and the Privacy Act of 1974.<sup>8</sup> This means, for example, that the Safeguards Rule<sup>9</sup> and the Privacy Rule<sup>10</sup> are likely to be subject to CFPB oversight, and new rules could be promulgated in those areas. As another example, under the Fair Credit Reporting Act, the CFPB is required to "identify patterns, practices, and specific forms of activity that can compromise the accuracy and integrity of information furnished to consumer reporting agencies," which could result in new rules regarding the data transfer or security.<sup>11</sup> A determination of the extent of authority over these issues that the CFPB will have, compared with other existing agencies, is just one of the issues that will likely develop over time; but in some cases the responsibility is clearer. For example, the Federal Trade Commission does not appear to be losing authority over items such as the Red Flags Rule and the Document Disposal Rule.<sup>12</sup>

## CFPB Privacy Responsibilities

While the new legislation still contains many unknowns, what is clear is that the CFPB will be deeply entrenched in privacy and data security issues. For example, covered persons must make available to consumers, upon request, "information in the control or possession of the covered person concerning the consumer financial product or service that the consumer obtained from such covered person, including information relating to any transaction, series of transactions, or to the account including costs, charges and usage data."<sup>13</sup> This information must be made available, unless exceptions apply, in an electronic form usable by consumers, so privacy and security concerns will be paramount.<sup>14</sup> Putting aside the broad rulemaking authority and explicit sections dealing with privacy rights and data access, there are also more nuanced privacy implications. For example, there are provisions governing the collection and disclosure of personally identifiable information that deserve close examination and will likely develop over time.<sup>15</sup>

## Privacy and Security Bills Percolating in Congress

In addition to the formation of this new agency, it is worth revisiting the several other bills that have been making their way around Congress, and worth highlighting other efforts that focus on privacy and data security issues. The Data Breach Notification Act (S. 139), introduced by Sen. Dianne Feinstein (D-Cal.) in early 2009, provides for a federal breach notification standard. Soon after the introduction of this bill, Rep. Bobby Rush (D-Ill.) introduced the Data Accountability and Trust Act (H.R. 2221) and Sen. Patrick Leahy (D-Vt.) reintroduced the Personal Data Privacy and Security Act (S. 1490). Rush's bill calls for information security policies, including requiring a process for disposing obsolete data. Leahy's bill also calls for a federal breach notification standard, but would also provide for making it a crime to intentionally or willfully conceal a security breach involving personal data.

A few months ago, Rep. Rick Boucher (D-Va.) introduced a privacy bill providing for a generally applicable privacy structure (as opposed to the existing U.S. sector-specific privacy legislation). Boucher's legislation calls for a high degree of privacy protection and transparency for the collection, use and sharing of information about consumers. The goal of the bill is to give consumers control over that collection, use and sharing, both online and offline. Then in June of this year, Howard A. Schmidt, the Cybersecurity Coordinator and Special Assistant to the President, introduced the draft National Strategy for Trusted Identities in Cyberspace, developed by the National Security Staff (NSS), and released it for public comment and input. The Strategy contains guiding principles and goals and objectives, including the goal to strengthen privacy protections for end-users and increase awareness of risks. The NSS is currently considering requiring identity-providers to abide by Fair Information Practice Principles, so this effort could result in best practices or legislative recommendations. The Department of Homeland Security (DHS), a key partner in the development of the strategy, has posted the draft NSTIC at <http://www.nstic.ideascale.com/>.

A few days ago, Sens. Tom Carper (D-Del.) and Bob Bennett (R-Utah) reintroduced legislation aimed at protecting consumers and businesses from identity theft and account fraud. The legislation, entitled the Data Security Act of 2010,

applies to financial institutions, retailers and government agencies, and would require these entities to: safeguard sensitive information, investigate security breaches, and notify consumers when there is a substantial risk of identity theft or account fraud. The proposed bill would also permit regulators to "levy fines, require corrective measures or even bar individuals from working in their respective industries" if they fail to disclose breaches adequately, according to the Senate's news release accompanying the bill.

## Stay Tuned: Legislative & Regulatory Kettles are Still Boiling

While uncertainty is in the air, especially as the CFPB gets up and running, privacy and data security and stewardship issues no doubt will be front and center for some time, and new laws and rules surely are on the horizon. With more than 200 rulemakings still to be issued as a result of the Dodd-Frank bill (24 of which will be issued by the CFPB), and a large number of research studies to be conducted, it is important to pay close attention to this rapidly developing area.

The Financial Industry Group at Reed Smith is kicking off a seven-part teleseminar series (invitation details to follow) in which various Reed Smith partners will focus on the impact of the legislation on:

Overview of the Dodd-Frank Bill – July 20 at 12 p.m. EDT, 90 minutes

The Derivatives Markets – July 27 at 12 p.m. EDT, 60 minutes

Executive Compensation and Corporate Governance – August 3 at 12 p.m. EDT, 60 minutes

Private Fund and Registered Fund Managers – August 10 at 12 p.m. EDT, 60 minutes

Consumer Protection and Privacy – August 17 at 12 p.m. EDT, 90 minutes

Enforcement and Litigation Trends – August 24 at 12 p.m. EDT, 60 minutes

Doing Deals and Raising Capital – August 31 at 12 p.m. EDT, 60 minutes

For more information contact, Christopher Cwalina , Mark Melodia, or Amy Mushahwar.

→ [Christopher G. Cwalina](#)  
Counsel,  
Washington, D.C.  
+1 202 414 9225

→ [Mark S. Melodia](#)  
Partner,  
Princeton  
+1 609 520 6015

→ [Amy S. Mushahwar](#)  
Associate, Washington, D.C.  
+1 202 414 9295



1 Section 1011.

2 Statement reported in various news outlets, including Huffington Post, 6/25/10. See also [financialservices.house.gov/Key\\_Issues/Financial\\_Regulatory\\_Reform/Conference\\_summaries/whatexperts\\_say.pdf](http://financialservices.house.gov/Key_Issues/Financial_Regulatory_Reform/Conference_summaries/whatexperts_say.pdf)

3 For example, the bill exempts those regulated by the Securities and Exchange Commission, the Commodity Futures Trading Commission and a state insurance regulator. Additionally, the bill has exempted auto dealers; real estate brokerage activities; accountants and tax preparers; the practice of law; employee benefit and other plans; persons regulated by a state securities commission; insurance; activities relating to charitable contributions; sellers of nonfinancial goods and services; and offering certain consumer financial products or services in connection with the sale or brokerage of nonfinancial goods or services. Some of these exemptions are limited in nature.

4 Section 1002.

5 Section 1031(b).

6 Id.

7 See, e.g., "ChoicePoint Settles Data Security Breach Charges; to Pay \$10 Million in Civil Penalties, \$5 Million for Consumer Redress," Press Release (Jan. 26, 2006 available at: <http://www.ftc.gov/opa/2006/01/choicepoint.shtm>)

8 Subtitle H.

9 16 CFR Part 314.

10 16 CFR Part 313.

11 Section 1088.

12 Under the definition of the enumerated consumer laws, the bill transfers: (F) the Fair Credit Reporting Act (158 U.S.C. 1681, et seq.), except with respect to sections 615(e) and 628 of that Act (15 U.S.C. 10 1681m(e), 1681w).

13 Section 1033.

14 A covered person is not required to disclose: "(1) any confidential commercial information, including an algorithm used to derive credit scores or other risk scores or predictors; (2) any information collected by the covered person for the purpose of preventing fraud or money laundering, or detecting, or making any report regarding other unlawful or potentially unlawful conduct; (3) any information required to be kept confidential by any other provision of law; and (4) any information that the covered person cannot retrieve in the ordinary course of its business with respect to that information."

<sup>15</sup> See, e.g., Sections 1022, 1071, 1094.

### About Reed Smith

Reed Smith is a global relationship law firm with nearly 1,600 lawyers in 22 offices throughout the United States, Europe, Asia and the Middle East. Founded in 1877, the firm represents leading international businesses, from Fortune 100 corporations to mid-market and emerging enterprises. Its lawyers provide litigation and other dispute resolution services in multi-jurisdictional and other high-stakes matters; deliver regulatory counsel; and execute the full range of strategic domestic and cross-border transactions. Reed Smith is a preeminent advisor to industries including financial services, life sciences, health care, advertising, technology and media, shipping, energy trade and commodities, real estate, manufacturing, and education. For more information, visit [reedsmith.com](http://reedsmith.com)

U.S.: [New York](#), [Chicago](#), [Los Angeles](#), [Washington](#), [San Francisco](#), [Philadelphia](#), [Pittsburgh](#), [Oakland](#), [Princeton](#), [Northern Virginia](#), [Wilmington](#), [Silicon Valley](#), [Century City](#), [Richmond](#)

Europe: [London](#), [Paris](#), [Munich](#), [Greece](#)

Middle East: [Abu Dhabi](#), [Dubai](#)

Asia: [Hong Kong](#), [Beijing](#)

© Reed Smith LLP 2010. All rights reserved.

Business from offices in the United States and Germany is carried on by Reed Smith LLP, a limited liability partnership formed in the state of Delaware; from the other offices, by Reed Smith LLP of England; but in Hong Kong, the business is carried on by Richards Butler in association with Reed Smith LLP (of Delaware, USA). A list of all Partners and employed attorneys as well as their court admissions can be inspected at the firm's website.

Attorney Advertising. This Alert may be considered advertising under the rules of some states. Prior results described cannot and do not guarantee or predict a similar outcome with respect to any future matter that we or any lawyer may be retained to handle.