Privacy and data security: the role of the US regulators

In the wake of the Dodd-Frank Wall Street Reform and Consumer Protection Act and in light of the rapid pace of innovation in the online and mobile payments industry, those involved in payment systems need to understand the US regulatory scheme for privacy and data security under which they operate. Additionally, those involved in the payments process need to understand which regulators have regulatory, examination, and enforcement authority with respect to each law, as Elizabeth E. McGinn, James T. Shreve and Alexander D. Lutch of BuckleySandler LLP discuss.

This article discusses the regulators and their jurisdiction, with a focus on the federal regulators having authority over many non-banks involved in payments products, such as the Consumer Financial Protection Bureau ('CFPB'), and the Federal Trade Commission ('FTC'). The article focuses on the Gramm-Leach-Bliley Act ('GLBA')[1] and the Fair Credit Reporting Act ('FCRA')[2] since these are key means through which the CFPB and FTC regulate privacy and data security practices. Although beyond the scope of this article, entities involved in payments products should also be aware of US anti-money laundering requirements, the impact of which may differ based on the role the entity plays in the payments process.

Scope of the federal privacy and data security laws

The requirements of GLBA, including privacy and safeguarding requirements, apply to entities that are 'financial institutions,' a term defined by reference to Section 4(k) of the Bank Holding Company Act ('BHCA'). Section 4(k) permits financial holding companies to engage in (1) activities financial in nature or incidental to such financial activity or (2) activity complementary to a financial activity that does not pose a substantial risk to the safety or soundness of depository institutions or the financial system generally[3]. This section of the BHCA permits the Board of Governors of the Federal Reserve ('FRB') to designate by rule permissible activities. The result is that entities 'significantly' engaged in activities found permissible for financial holding companies are financial institutions and subject to the requirements of GLBA. Although many entities involved in the payment process likely qualify as financial institutions, some may perform services that do not meet the BHCA test.

The requirements of FCRA revolve around information constituting a 'consumer report.' The term 'consumer report' is broadly defined, subject to certain exclusions, to include 'any written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer's eligibility for: (A) credit or insurance to be used primarily for personal, family, or household purposes; (B) employment purposes; or (C) any other purpose authorized under section 1681b of [FCRA].'[4] FCRA imposes requirements relating to the compilation, use, sharing and disposal of consumer reports and, in some cases, information derived from consumer reports. Of note to those involved in payments systems are limitations on the use for marketing purposes of 'eligibility information' received from affiliated entities.

The Consumer Financial Protection Bureau

The CFPB has the authority to 'regulate the offering and provision of consumer financial products or services under the Federal consumer financial laws.'[5] The CFPB can prohibit practices it finds to be unfair, deceptive or abusive ('UDAAP') and mandate particular disclosures relating to financial products or services. CFPB authority includes supervisory and rulemaking authority over 'any person that engages in offering or providing a consumer financial product or service' and any affiliate of such a person if the affiliate acts as a service provider to the person[6].

The definition of 'consumer financial product or service' includes 'providing payments or other financial data processing products or services to a consumer' with certain exceptions. The CFPB also has the authority to define products or services that fall within its jurisdiction if it determines that the product or service is (1) designed to avoid any federal consumer financial law and (2) would be a permissible product for a bank or financial holding company to offer and has a material impact on consumers[7]. This provision of DFA appears to provide the CFPB with authority beyond the scope of GLBA or FCRA to cover entities that are not technically a financial institution, as may be the case for some entities in payment systems. Although supervisory authority over depository institutions remains with the federal bank regulatory

agencies, supervisory authority over certain non-depository institutions is given to the CFPB.

Privacy and data security compliance post-DFA

Included among the Dodd-Frank Wall Street Reform and Consumer Protection Act ('DFA') list of laws over which authority is transferred to the CFPB are certain privacy provisions of the GLBA and FCRA. In general, one may characterise the DFA treatment of privacy and data security regulation as splitting the two areas with privacy regulation (the limitations on the dissemination and use of information) being transferred to the CFPB and information security regulation (such as information safeguarding and disposal requirements) remaining with the current regulators. The retention of information security jurisdiction by the existing regulators may be, in part, due to the banking regulators' retention of bank safety and soundness matters. Privacy may have been seen as more of a consumer protection concern within the bailiwick of the CFPB.

What the Consumer Financial Protection Bureau has done

Since the agency's establishment, regulatory action in the area of privacy has consisted primarily of the reissuance of regulations promulgated by other financial regulators under the authority of GLBA and FCRA as Regulations P and V respectively. The CFPB regulations do not substantively change the prior requirements[8].

The CFPB has incorporated the agency's examination authority over privacy into its standard examination materials, with privacy being a stand alone module. The privacy module inquires about a financial institution's GLBA privacy notice, opt-out procedures, and consumer preferences tracking. Notably for those in the payments space, the CFPB has used its examination authority to review compliance by many entities not previously regulated at the federal level and less familiar with the rigor of federal compliance examinations.

In spite of the regulatory restructuring under DFA, privacy, particularly with mobile payments and applications, remains a primary focus of the FTC.

Some commentators have expressed concern that the potentially expansive scope of CFPB's UDAAP enforcement authority could be used to examine entities' data security practices and initiate enforcement actions. The agency's Supervision and Examination Manual instructs examiners to inquire about the results of any data security examination under GLBA, though the manual notes that the information should be 'used to determine the accuracy of the institution's privacy disclosures regarding data security.'[9] While the CFPB has not yet announced any enforcement actions under its UDAAP authority regarding data security, companies should be aware that the agency will possess compliance information regarding data security that could be used to initiate a UDAAP claim.

Federal Trade Commission action since DFA

Although the FTC no longer is specifically vested with authority over privacy practices in regard to many financial institutions over whom the agency had authority prior to DFA, the agency has remained active in data security regulation and enforcement as well as retaining the general authority to prevent unfair or deceptive acts and practices. The FTC has also shown considerable interest in new payment systems, particularly mobile payments. Since the transfer of certain privacy authority to the CFPB, the FTC has issued several staff reports involving privacy. These include a report on consumer protections (including those for privacy and data security) in mobile payments and a report on privacy disclosures on mobile devices which focuses primarily on online privacy notices that are required under California law and recommended by the FTC. Notably, the report on privacy disclosures, while focused primarily on the California law, also mentions GLBA privacy notices. These actions make clear that in spite of the regulatory restructuring under DFA, privacy, particularly with mobile payments and applications, remains a primary focus of the FTC.

Regulation by contract

Non-banks involved in payment systems may also find that banks are imposing, by contractual means, bank privacy and information security requirements, which are often more stringent than those applicable to non-bank entities. Banks are generally held responsible for the privacy and data security practices of those deemed 'service providers' of the bank. As a result, while a non-bank entity may not by law be subject to certain regulatory requirements, a bank's own compliance obligations may require the bank to pass the requirements to other entities.

Elizabeth E. McGinn Partner
James T. Shreve Attorney
Alexander D. Lutch Attorney
BuckleySandler LLP
emcginn@buckleysandler.com
jshreve@buckleysandler.com
alutch@buckleysandler.com

1. 15 U.S.C. § 6801 et seq.
2. 15 U.S.C. § 1681 et seq.
3. 12 U.S.C. § 1843(k).
4. 15 U.S.C. § 1681a(d)(1).
5. 12 U.S.C. § 5491.
6. 12 U.S.C. § 5481.
7. 12 U.S.C. § 5481(15).
8. See, 76 Fed. Reg. 79,026 (Dec. 21, 2011).
9. CFPB Supervision and Examination Manual v.2 - Examination Procedures - GLBA Privacy, Procedures pp. 2-3.