Examining the Extensive Regulation of Financial Technologies

July 2016

About Financial Innovation Now

Financial Innovation Now is an alliance of technology leaders, including Amazon, Apple, Google, Intuit and PayPal, that are working together to modernize the way consumers and businesses manage money and conduct commerce. We believe that technological transformation will make financial services more accessible, safe and affordable for everyone, and we promote policies that enable these innovations. To learn more, visit: http://financialinnovationnow.org.

Executive Summary

Technology and innovation are fostering change in nearly every aspect of financial services today and bringing significant benefits to both businesses and consumers. As is the case with many industries threatened by technological transformation, some have called for greater regulation of new entrants to the marketplace, arguing that new technologically advanced services somehow face fewer regulations and unfairly benefit from an un-level playing field. However, the reality is quite the opposite. Financial technology innovators' products and services are heavily regulated. In fact, current regulatory compliance requirements constitute a significant market barrier for any new entrant in financial services, and sometimes serves to protect incumbent providers from new competition.

This paper summarizes the regulatory environment for two new categories of financial services: online lending and emerging payments technologies. It describes two hypothetical innovators: 1) a payments security technology and, 2) an alternative small business lending service. For both of these innovators, the paper narrates the regulatory hurdles confronting a product that falls into the sphere of financial services. It then details the laws and regulations that affect payments and lending. Finally, this paper provides an overview of the comprehensive regulatory scheme covering data security as well as the laws governing consumer protection, anti-money laundering that apply to these new entrants.

This paper does not argue against the goals of financial regulations, rather it seeks merely to provide policymakers with a brief overview of the current regulatory landscape confronting new financial services providers.

Introduction

Financial services and products comprise one of the most regulated sectors in the American economy. Any new financial service or product must comply with most, if not all, of this regulatory regime. As in other markets, technology companies have entered the financial services space and brought with them new and innovative ways to make payments, lend money, lower costs and increase choices for consumers and businesses. Unlike in other markets, however, innovators in financial services must devote significant time and resources to regulatory compliance that can chill investment and innovation or slow time to market - ultimately harming consumers and businesses that benefit from easier access and more affordable services. While many of the regulations are necessary to protect consumers, small businesses and the economy, some regulations are redundant, conflicting or antiquated. Further, new technologies may themselves solve regulatory policy goals and obviate the need for some regulations. In other cases, modernizing regulations may enable maximum benefit from modern technology, the internet and mobility.

Payment and lending innovators, in particular, are not only subject to direct regulation from a number of federal and state regulators, but also face flow-down regulation as a result of doing business with depository institutions and credit card companies. These new financial services providers may also face additional threats of private liability for even technical violations of some rules and regulations, including class actions that could threaten to impose significant damages. As a result of these pressures, as well as competitive, market and reputational incentives, payment processors and non-bank lenders invest millions of dollars in security and sophisticated compliance programs to meet customer expectations and follow all applicable rules and requirements.

Regulation impacts every aspect of the online lending process, from customer acquisition and disclosures to data security, underwriting and debt collection. As the hypothetical examples and the legal summaries below illustrate, there is no disparity between banks and non-bank lenders and processors in the regulation of the relevant areas of risk. Likewise, regulation is ubiquitous for payment processors; affecting their on-boarding of merchants, their protection of the data they transmit, their monitoring of transactions and charge-backs and numerous other aspects of their operations.

The regulatory environments in which banks and these new lenders and processors operate have differences, but those differences are due to their very different business models. In relevant risk areas the regulations are the same or equally rigorous. The current system of bank regulation was enacted in the early 1930s and, until recent years, was focused primarily on preventing losses to the Federal Deposit Insurance Corporation ("FDIC") insurance fund.

Bank regulators' primary concern, therefore, was creating an elaborate system of safety and soundness regulation to limit the financial risks that they permitted federally insured institutions to take. Over time, Congress came to understand that bank holding companies posed similar risks to the FDIC and brought them under the same type of safety and soundness regulatory structure. Throughout this period, banks and commercial companies were kept separate, in recognition that the trade-off for the low-cost funding offered by federal deposit insurance was that banks should be run very conservatively and not permitted to put the government's funds at risk.

With the financial collapse of large financial firms like Bear Sterns, AIG and Lehman Brothers, the financial crisis of 2007-2008 broadened Congress' concern about the types of financial institutions that could pose risks to federal taxpayers. The Dodd Frank Act addressed these risks by creating a category of "Systemically Important Financial Institutions," known as SIFIs, that were brought within the federal safety and soundness regime. However, Congress did not include other financial institutions that did not pose significant financial risks to federal taxpayers in this regulatory scheme. For example, Congress did not find a systemic risk to the economy from mortgage brokers and bankers, other non-bank lenders, payments and credit card companies, credit reporting agencies, appraisers, title insurers, escrow agents, pawn shops, or a host of other businesses that provide financial services to consumers and businesses. Therefore, these businesses are purposefully not subject to the enhanced safety and soundness regulatory structure that applies to banks and SIFIs.

Congress has determined that only banks and SIFIs should be subject to a federal safety and soundness regime. However, an elaborate legal and regulatory structure, intended to protect consumers, ensure data security and prevent money laundering and financing of terrorist activities, governs lending and payment companies. This structure, described in some detail below, includes both federal regulators and a patchwork of state regulators. Although well intended, the underlying laws, regulations and regulatory interpretations are often slow to adapt to technological change, creating barriers to innovators who wish to bring new products and services to market.

This system is supported by some incumbent players to benefit from anachronistic barriers to entry, and these entities may resist regulatory modernization. Some may even urge the adoption of additional and unnecessary burdens on innovative new entrants such as a federal safety and soundness regulatory regime like that imposed on banks and SIFIs - ignoring the fact that these new entrants pose no significant financial risk to taxpayers.

Online Lending

A) New Lending Service Meets Unserved Needs: "LendNow"

Technology companies are bringing rapid changes to the lending marketplace and some of these innovations have forced change in processes that have remained static for decades. These changes have brought significant benefits to consumers and the economy by reducing transaction costs; improving speed and convenience; increasing competition, consumer choice and transparency; and bringing reasonably priced credit to consumers and businesses that have not been served adequately by traditional financial institutions. However, the regulatory and legal barriers to entering the lending business in the United States are very high.

To demonstrate, take the hypothetical example of an established payment processing company that wishes to provide small business loans to its merchant customer base online. This new service will be referred to as "LendNow." Payment processors enable commerce by permitting merchants to convert their customers' payments into deposits in their bank accounts. Because merchants are the processors' clients, the processors have a comprehensive understanding of the merchants' income, cash flows, inventory (if necessary) and/or other business operations. Thus, LendNow is generally in a better position than traditional financial institutions to quickly conduct a risk assessment and underwrite small loans to these merchants. Applications can often be prepopulated and completed online in minutes. Underwriting is automated, with approvals sometimes the same day or within 2-3 days and funds deposited soon after into the merchant's account. LendNow can also arrange repayment from the merchant's payments stream that it handles.

This new type of lending product offers many benefits to small business owners. First, banks and other traditional lenders simply do not find it profitable to make and underwrite small loans because the cost of underwriting makes it impossible to offer them at reasonable rates.[1] Without access to banks, these small business owners often exhaust all other forms of credit (including loans from family and friends) and might even be forced to turn to less traditional sources of quick credit such as payday lenders. However, LendNow can make relatively small loans at reasonable rates: Its processing costs are low due to the online nature of its business, and highly reliable information needed to make a well substantiated

[1] According to one study, transaction costs to process a $100,000 loan are comparable to those to process a $1 million loan. Karen Gordon Mills, Brayden McCarthy, The State of Small Business Lending: Credit Access During the Recovery and How Technology May Change the Game, Harvard Business School Working Paper 15-004 (July 22, 2014) at 6, 11, 12 and 28.

underwriting decision is already in its systems - unlike long written applications that are prone to misrepresentation and error and require a lengthy verification process.

Second, the loans can be made quickly. The innovative technology that LendNow has developed permits almost instantaneous underwriting, and LendNow's position as a payment processor permits it to fund the loan quickly. This advantage is important to many small businesses that need quick credit to fund temporary cash flow shortages, replace broken equipment, or deal with other problems that could close down or impair their businesses and cause them losses that would far exceed the cost of the credit.[2]

Third, the time and effort required of the small business to apply for the loan is minimal. To busy entrepreneurs, their own time is critical and the ease of applying for credit from their familiar payments processor is a significant advantage. LendNow's new online lending application takes just minutes to complete. By comparison, small business owners report spending an average of 24 hours applying for credit from traditional banking sources.[3]

It seems like LendNow should be in a great position to begin making small business loans - but it must run a regulatory gauntlet before it can do so.[4]

The first hurdle to any lender that is not a bank is the patchwork of state lending laws it must face. The problem for any non-bank lender, but particularly for online lenders is that every state has its own lending laws, including its own registration requirements, license fees, training requirements, staffing rules, etc. Many of the state regulations do not account for innovation or technology changes. An online lender, which by the nature of its business model usually serves borrowers in many or all states, must generally comply with all of them. These state laws often were written for mortgage lending and LendNow, will now need to comply with requirements for mortgages even though LendNow will not be financing any mortgages.

Registering, becoming licensed and complying with multiple state systems is a complex process, as some of the state regulations place a significant compliance burden on online lending platforms that operate across state lines. If our hypothetical lender wants to loan to small businesses in California, for example, it must be licensed in that state and post a bond.

---

[2]Non start-up small business owners report that their largest challenge is uneven cash flow. Federal Reserve Banks of New York, Atlanta, Cleveland and Philadelphia, *Joint Small Business Credit Survey Report*, 2014 at 9 (released February 2015) (*Joint Small Business Credit Survey Report*).

[3]*Id.* at 4.

[4] LendNow is not lending to individual consumers. If it did, its business model would also have to deal with numerous other laws and regulations intended to protect consumers. They are detailed in the section on Regulatory Requirements Facing the Online Lending Industry, below. Among them are the Truth in Lending Act ("TILA") and Regulation Z ("Reg Z") (which include both disclosure and know-your-customer requirements), the Fair Credit Reporting Act ("FCRA") (governing supply and use of data provided by and to credit reporting agencies and permissible use of consumer reports), the Fair Debt Collection Practices Act ("FDCPA") (governing collection practices), the Electronic Funds Transfer Act ("EFTA") and Regulation E ("Reg E") (disclosure related to automated debits and transfers), and state consumer protection laws too numerous to list.

It must make its records available to state examiners, stay up to date on numerous disclosure rules and pay the expenses of California examiners to travel to its facilities wherever in the country they may be. Each state and the federal government uses a different definition for the same terms. California, for example, defines a commercial loan under $5,000 as a consumer loan - a nuance that could easily trip up online lenders making small business loans.[5] Thus, reducing a commercial loan from $5,000 to $4,999.99 exposes an online lender to an entire additional chapter of the California Code, with many dozens of additional restrictions and requirements.[6] The California statute also includes detailed provisions requiring that the California Commissioner of Banking approve any businesses that are to be co-located with the lender's office, and requires separate licenses for separate locations.[7] These requirements clearly do not contemplate modern lending, which can be done entirely online by lenders located out of state and without a single physical "location" that is negotiating with a borrower.

The complexity of dealing with so many different and confusing state legal systems represents a costly market barrier that delays entry of new, affordable products. Instead, many online lenders choose to partner with a national bank to issue the loans and, therefore, the loans are subject to the same regulatory and supervisory framework applicable to the issuing bank. LendNow, therefore, must find one or more bank partners that will make the loans under the bank's name, even if our lender provides the lending platform and may also assume the risk of the loans by purchasing them from the bank. However, by bringing an FDIC insured bank into the product offering, LendNow will also assume some additional regulatory burdens. Now it has subjected itself to examination by examiners from the Office of the Comptroller of the Currency and the Federal Deposit Insurance Corporation, because it is considered a third-party service provider to the bank.[8] Even though LendNow purchased the loans from the bank, the examiners may worry that there might be risks in the new lending platform that could create liability to the bank. Therefore, LendNow must open up its underwriting processes to examination by bank regulators and periodic audits by the bank to make sure that it does not create a risk to the bank. It is subject to guidance documents from those agencies (detailed in the section on "Regulatory Requirements Facing the Online

[5] Cal. Fin. Code § 22204.

[6] *See* Cal. Fin. Code Chapter 2. Consumer Loans.

[7] Cal Fin. Code §§ 22102, 22152, and 22154**.**

[8] "Service provider" means

> any person that provides a material service to a covered person in connection with the offering or provision by such covered person of a consumer financial product or service, including a person that - (i) participates in designing, operating, or maintaining the consumer financial product or service; or (ii) processes transactions relating to the consumer financial product or service (other than unknowingly or incidentally transmitting or processing financial data in a
> manner that such data is undifferentiated from other types of data of the same form as the person transmits or processes) . . . .

12 U.S.C. § 5481(26); Office of the Comptroller of the Currency ("OCC") Bulletin 2013-29 (Oct. 30, 2013) available at: http://www.occ.gov/news-issuances/bulletins/2013/bulletin-2013-29.html (Guidance regarding all third party relationships, including service providers).

Lending Industry," below) that closely govern its operations and require the bank to audit and document the safety and soundness of its finances as well as its loan platform.

Even without the bank partnership, however, LendNow must comply with many of the same regulations that are applicable to the bank. It is subject to Equal Credit Opportunity Act (ECOA) and must test its systems to make sure they do not have a discriminatory impact against small businesses owned by minorities, women or other protected categories. LendNow must also establish controls, policies and procedures and set up a compliance function to help ensure it complies with the Customer Identification Program requirements of the Treasury Department and make sure it is not being used to launder money or finance terrorism.

LendNow is also a payment processor, which means that it has experience and deep expertise in data security. As detailed in the "Regulatory Requirements With Which a New Payments Service Must Comply" section below, payment processors must comply with the Payment Card Industry Data Security Standard ("PCI DSS"), a set of detailed requirements that apply to all participants in the credit card process that handle sensitive personal data. Like banks, LendNow also has experience with and has long been subject to the privacy, data security and breach notification provisions of the Gramm-Leach Bliley Act ("GLBA") and its implementing regulations, including Regulation P ("Reg P"), which apply to all financial firms.

LendNow also has experience complying with other regulatory requirements to which its new product will be subject, though it will still need additional time and money to comply. As a payments company, it has a deep understanding of the Bank Secrecy Act ("BSA") and anti-money laundering ("AML") regulations and is particularly experienced in spotting credit card laundering schemes. Nevertheless, the new online lending product will require expansion of its compliance department and new policies, procedures and controls to deal with risks unique to that business. Processors have also long come within the jurisdiction of the Federal Trade Commission ("FTC") to prevent unfair and deceptive acts or practices ("UDAP") and anticompetitive behavior under the FTC Act. Here again, its compliance department will need to update its compliance management system for the new business line. LendNow will also need to study and at times, implement some of the consumer lending laws, such as the Fair Credit Reporting Act ("FCRA"), Fair Debt Collections Practices Act ("FDCPA") and Electronic Funds Transfer Act ("EFTA") to make sure its business model does not impact consumers in a way that might bring these regulatory schemes into play.

Having beefed up its compliance department, drafted and distributed new policies and procedures, implemented new controls and trained its staff and management who will be involved in lending, our new online lender is ready to start making loans. At this point, as discussed above, partnering with a bank provides some benefit to LendNow, so it will now likely want to seek out a bank partner. However, persuading a bank partner to use the new platform will be difficult because the bank will first want the potential partner to vet its

product with the appropriate regulators. For this reason, our new lender is well advised to visit the Consumer Financial Protection Bureau ("CFPB") and the traditional banking regulators (hopefully, with its prospective bank partner) to present and explain its system to them and make sure they understand how it works. This discussion not only helps pave the way to partner with a bank by dealing with regulators' likely concerns before a product is launched, but helps reduce the risk of receiving a civil investigative demand ("CID") or notice of a special examination from a skeptical regulator shortly after the product launch.

B) Regulatory Requirements Facing the Online Lending Industry

Online lenders are subject to the same federal lending laws as banks. Unless they partner with banks, they are also subject to greater state regulation than many banks, which can operate across state lines without regard to local lending laws.[9] The following laws are among those generally applicable to online lenders:

- *The Equal Credit Opportunity Act ("ECOA") and Regulation B*

  ECOA prohibits discrimination in lending on the basis of race and other protected categories.[10] The Regulation includes numerous requirements and prohibitions, and failure to comply brings the risk of enforcement actions by regulators and private litigation. Regulation B also imposes extensive record retention requirements on lenders.[11]

  ECOA and Regulation B require significant compliance resources and create litigation and enforcement risks that lenders can only partly control. For example, the CFPB and the Department of Justice have taken the position that policies or practices that have a discriminatory impact are prohibited under ECOA, even if the impact was unknown and unintended.[12] Because the lenders cannot collect statistical information about the protected statuses of borrowers,[13] the agencies use surnames and zip codes as a "proxy" for race to determine if protected groups are denied or charged more for credit than others. If the agencies think there are statistical disparities, they may bring an enforcement investigation. Therefore, ensuring that its lending program does not cause unintentional violations of ECOA may require an online lender to proactively assess the non-discriminatory impact of its lending program, and may require a

[9] Recently, the validity of certain partnership arrangements has been called into question by an appellate court decision that prevents purchasers of bank debt from availing themselves of the bank's power to avoid state usury laws. *Madden v. Midland Funding, LLC*, 786 F.3d 246 (2d Cir. 2015), *cert. denied*, 579 U.S. _ (June 27, 2016).
[10] 15 U.S.C. 1601 et seq., 12 C.F.R. part 1002.
[11] 12 C.F.R § 1002.12.
[12] *In the Matter of Ally Financial Inc.; and Ally Bank*, Administrative Proceeding File No. 2013-CFPB-0010, Consent Order, Consumer Financial Protection Bureau (Dec. 19, 2013), available at http://files.consumerfinance.gov/f/201312_cfpb_consent-order_ally.pdf.
[13] 12 C.F.R § 1002.5(b).

periodic retroactive statistical analysis of a lender's portfolio to attempt to ascertain the gender and racial mix of the borrowers.

- *Gramm Leach Bliley Act (GLBA), Privacy of Consumer Financial Information and Regulation P*

  GLBA requires financial institutions to provide data security, breach notification and privacy and data sharing protections to consumers.[14] The Federal Trade Commission (FTC), the Consumer Financial Protection Bureau (CFPB) and each federal bank regulatory agency (Agency), have all issued slightly different regulations governing the treatment of nonpublic personal information (NPI) about consumers by financial institutions (collectively, the Privacy Rules).[15]

  The Privacy Rules generally require "financial institutions" to provide notice to customers (and other consumers in some circumstances) about their privacy policies and practices; describe the conditions under which financial institutions may disclose nonpublic personal information to nonaffiliated third parties; and provide a method for consumers to prevent financial institutions from disclosing that information to most nonaffiliated third parties by "opting-out" of that disclosure, subject to certain exceptions.[16] Under the Privacy Rules, online lenders are considered "financial institutions"[17] and therefore subject to these requirements.

- *GLBA and Customer Information Security Guidelines*

  Online lending companies are considered "financial institutions" subject to guidelines for safeguarding nonpublic personal information about customers that the FTC and the banking agencies have adopted to implement Sections 501 and 505(b)(2) of the GLBA (15 U.S.C. §§ 6801(b) and 6805(b)(2)).[18]

---

[14] 15 U.S.C. § 6804.

[15] 16 C.F.R. Part 313; 12 C.F.R. Part 1016; 12 C.F.R. Part 332; 12 C.F.R. Part 216; 12 C.F.R. Part 40; 12 C.F.R. Part 573.

[16] 16 C.F.R. § 313.1(a); 12 C.F.R. §1016.1(a); 12 C.F.R. §§ 332.7, 332.10; 12 C.F.R. §§ 216.7, 216.10; 12 C.F.R. §§ 40.7, 40.10; 12 C.F.R. §§ 573.7, 573.10.

[17] For purposes of the Privacy Rules, a financial institution includes "any institution that is significantly engaged in financial activities or incidental to such financial activities as described in section 4(k) of the Bank Holding Company Act of 1956, as amended [12 U.S.C. § 1843(k)(4)]." Sec 4(k) offers a broad description of what constitutes "activities that are financial in nature" including "Lending, exchanging, transferring . . . money or securities" and "Providing financial, investment, or economic advisory services." Id. Payment processing is a core banking function and is at the very least "incidental" to transferring funds or providing credit. *See* 12 CFR 225.28 (the term includes "any activity usual in connection with making, acquiring, brokering or servicing loans or other extensions of credit, as determined by the Board"). Although the Federal Reserve Board does not specifically list payment processing among its examples, that is probably because it is a core banking function, not an activity as to which there would be any question.

[18] For purposes of the Guidelines, a financial institution means "any institution that is significantly engaged in financial activities as described in Section 4(k) of the Bank Holding Company Act of 1956, as amended;" a service provider means "any person or entity that maintains, processes, or otherwise is permitted access to customer information through its provision of services directly to the bank (emphasis added);" and customer information means "any record containing nonpublic personal information as defined in the [Privacy Rules] about a customer of a [financial institution], whether in paper, electronic, or other form, that is handled or maintained by or on behalf of [the financial institution] or [its] affiliates." 16 C.F.R. §§ 314.2(a), (b), (d), 314.3(b), (k)(1); See also, 12 C.F.R. Part 364, Appendix B, Section I; 12 C.F.R. Part 208, Appendix D-2, Section I; 12 C.F.R. Part 30, Appendix B, Section I; 12 C.F.R. Part 570, Appendix B, Section I..

The Guidelines require lenders to develop, implement and maintain comprehensive written information security programs designed to ensure the security and confidentiality of customer information; to protect against any anticipated threats or hazards to the security or integrity of such information; and to protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer.[19] The Guidelines also generally require lenders to exercise appropriate due diligence in selecting service providers; require service providers by contract to implement appropriate measures designed to meet the guidelines' objectives; and monitor the service provider's compliance with these obligations such as by reviewing audits, summaries of test results and other equivalent evaluations of its service providers.[20] Finally, as part of the security program proscribed by Section 501(b) of the GLBA, financial institutions must establish a breach response program with an incident response team that will notify affected customers when a breach occurs; ensure that third party service providers are taking appropriate measures to secure data and respond to a security incident; and involve law enforcement in a timely manner.

- *GLBA and the FTC's Safeguards Rule*

  Online lenders are financial institutions subject to the FTC's Standards for Safeguarding Customer Information ("Safeguards Rule"), which have been codified at 16 C.F.R. Part 314. The Safeguards Rule requires all financial institutions over which the Federal Trade Commission has jurisdiction to develop and maintain a comprehensive information security program to safeguard "customer information" - which is defined as any record containing non-public personal information.

  Subject institutions are required to designate an employee to coordinate the information security program, identify foreseeable security risks, design and implement safeguards to control the risk and test and evaluate the program. In addition, the Safeguards Rule requires subject institutions to ensure that service providers with access to customer information implement and maintain sufficient security measures.

- *Bank Secrecy Act and Anti Money Laundering Regulations*

[19] 12 U.S.C. § 3401(1); 16 C.F.R. § 314.3; 12 C.F.R. Part 364, Appendix B, Section II; 12 C.F.R. Part 208, Appendix D-2, Section II. 12 C.F.R. Part 30, Appendix B, Section II; 12 C.F.R. Part 570, Appendix B, Section II.

[20] *See, e.g.*, 12 C.F.R. Parts 364 (Appendix B), 208 (Appendix D-2), 30 (Appendix B), 570 (Appendix B). *See also* Section III.D. of Appendix B to 12 C.F.R. Part 30.

The Bank Secrecy Act and its implementing regulations ("BSA Rules") are a mechanism by which the United States government combats drug trafficking, money laundering and other crimes.[21] The BSA Rules were enacted primarily to prevent banks and other financial service providers from being used as intermediaries for, or to hide the transfer or deposit of money derived from, such criminal activity.[22] The Rules identify transactions and circumstances that must be reported to federal authorities, and define compliance systems that must be employed.

- *Regulation E, the Electronic Funds Transfer Act (EFTA*)

  The Electronic Funds Transfer Act ("EFTA") and it's implementing rule, Regulation E (collectively "EFT Laws"), provide a basic framework for establishing the rights, liabilities and responsibilities of consumers who use electronic fund services and of financial institutions and certain other persons that provide consumers with electronic fund services.[23] Under the EFTA, funds can be transferred by way of an electronic terminal, a telephone, a computer or magnetic stripe for the purpose of ordering or authorizing a financial institution to debit or credit a consumer's account. A primary focus of Regulation E, which is issued by the CFPB, is disclosures that must be made to customers who authorize electronic payments from their accounts.[24] Therefore, lenders that allow for electronic payments or debits must make sure to provide all such relevant notices. Additionally, EFTA governs, among other things, how and when a financial intuition or online lender may set up an automatic debit of a consumer's account. Online lenders must establish a program to ensure compliance with EFTA and Regulation E.

- *Electronic Signatures Act (E-SIGN)*

  E-SIGN allows electronic documents and signatures to have the same validity and effect as paper documents and handwritten signatures, and was designed to facilitate remote banking and approval.[25] After obtaining proper consent under the E-SIGN Act, financial institutions can provide most written disclosures in electronic form.[26] E-SIGN requires that prior to obtaining consent, financial institutions must provide a clear and conspicuous statement informing the consumer of their rights to a paper copy of their records, to withdraw consent, and any conditions or limitations of their consent. The Federal Reserve Board has established uniform standards for electronic delivery of federally mandated disclosures related to Equal Credit Opportunity (Regulation B); Electronic Fund Transfers (Regulation E); Consumer Leasing (Regulation M); Truth in

[21] 31 U.S.C. § 5311-5330, 12 U.S.C. § 1829b, §§ 1951-1959; USA PATRIOT ACT, 31 U.S.C. § 5312(a)(2) (expanding the AML program); 31 C.F.R. Title X.
[22] *See, e.g.,* 31 U.S.C. §§ 5313(a) and 5318(g).
[23] 15 U.S.C. §§ 1693 et seq.; 12 C.F.R. Part 1005.
[24] *See* 12 C.F.R. § 1005.9(a).
[25] *Electronic Signatures in Global and National Commerce Act*, 15 U.S.C. § 7011 et seq. (2000).
[26] *See* 72 Fed. Reg. 63,452 (Nov. 9, 2007) (electronic delivery rules for disclosures required under Regulation E).

Lending (Regulation Z); and Truth in Savings (Regulation DD).[27] E-SIGN also mandates that companies comply with the Act's record retention requirements.

- *Unfair, Deceptive and Abusive Acts or Practices (UDAAP) prohibition*

  Title X of the Dodd-Frank Act, akin to the FTC Act, prohibits covered persons and service providers from engaging in unfair, deceptive, or abusive acts or practices.[28] It further prohibits any person from knowingly or recklessly providing substantial assistance to covered persons and service providers that engage in such practices.[29] Online lenders, like financial institutions, are subject to UDAAP enforcement. The CFPB has not clearly established rules and standards as to what constitutes a UDAAP violation, but have instead chosen to define the parameters of this law by publicizing enforcement actions against companies it views as violators.[30] UDAAP actions may be brought for a variety of deceptive, abusive, or unfair violations of the law. Recently, the CFPB brought its first UDAAP action against an online lender for failing to provide adequate data security practices.[31]

- *Fair Debt Collection Practices Act (FDCPA)*

  The FDCPA prohibits deceptive, unfair and abusive collection practices.[32] The law is targeted at third-party debt collectors, including purchasers of defaulted debt. Guidance from bank regulators makes clear that lenders cannot avoid responsibility for collection practices on consumer debt by selling it.[33] The FDCPA applies to debt incurred primarily for personal, family, or household purposes - not commercial debt. While the FDCPA may not apply directly to online consumer lenders that collect their own debt, lenders are generally required by regulators to undertake extensive audits of and monitoring of their third party debt collectors. The compliance requirements of the FDCPA are particularly difficult for online lenders that operate with bank partners, because the online lender not only has to complete its own audit of any third-party

[27] Rules and Regulations, Federal Register, Vol. 72, No. 217 (Nov. 9, 2007) 72 FR 63445-63452 (Equal Credit Opportunity, Regulation B); 72 FR 63452-63456 (Electronic Fund Transfers, Regulation E); (72 FR 63456-63462 (Consumer Leasing, Regulation M); 72 FR 63462-63477 (Truth in Lending, Regulation Z); 72 FR 63477-63484 (Truth in Savings, Regulation DD).
[28] 12 U.S.C. § 5531.
[29] 12 U.S.C. § 5536(a)(3).
[30] CFPB Director Richard Cordray announced the precedential value of seeking to glean guidance from previous consent orders, saying that "it would be 'compliance malpractice' for executives not to take careful bearings from the contents of these orders about how to comply with the law and treat consumers fairly." Prepared Remarks of CFPB Director Richard Cordray at the Consumer Bankers Association (March 9, 2016), available at http://www.consumerfinance.gov/newsroom/prepared-remarks-of-cfpb-director-richard-cordray-at-the-consumer-bankers-association/.
[31] *In the Matter of Dwolla, Inc.*, Administrative Proceeding File No. 2016-CFPB-0007, Consent Order (Feb. 27, 2016) available at http://files.consumerfinance.gov/f/201603_cfpb_consent-order-dwolla-inc.pdf.
[32] 15 U.S.C. § 1692 et seq.
[33] *See, e.g.,* OCC Bulletin 2014-37 (Aug. 4, 2014) (requiring strict monitoring and controls of debt buyers by national banks that sell debt), available at http://www.occ.gov/news-issuances/bulletins/2014/bulletin-2014-37.html.

collection agency it may use, but must anticipate that its bank partner may also need to audit the debt collector service provider.[34]

- *Telephone Consumer Protection Act*

  The TCPA restricts telephone solicitations and limits the use of robocalls (made by way of an automatic dialing system), artificial or prerecorded voice messages, SMS text messages and junk faxes.35 It also specifies several technical requirements for fax machines, auto dialers and voice messaging systems, including identifying the entity using the device. To the extent that a payment processor or any of its vendors telemarket services or products to consumers, or use autodialers or prerecorded or artificial voice messages to communicate with consumers, they are subject to the Telephone Consumer Protection Act ("TCPA"). The TCPA is a law that applies to all entities that engage in telemarketing or the use of autodialers or prerecorded or artificial voice messages to reach consumers. The law is implemented and generally enforced by the Federal Communications Commission ("FCC"), although a subdivision of the law, the Do Not Call rule (see below), is enforced by the Federal Trade Commission ("FTC").[36] The law also imposes time-of-day restrictions for placing telemarketing calls (between 8 AM and 9 PM local time), outlines procedures for the FTC's Do Not Call Registry and grants consumers a private right of action.[37]

  With respect to voice calls, the TCPA prohibits a caller from initiating any call to a cell phone or wireless number that was autodialed, or initiating a call that includes a prerecorded or artificial voice without an emergency, or the prior express consent of the recipient (current subscriber or customary user). Any such calls placed to a cell phone that constitute telemarketing require "prior express written consent" from the recipient.[38]

  Calls made to residential lines that include a prerecorded, or artificial voice are prohibited without the "prior express written consent" of the recipient unless the call is made for emergency purposes; not made for commercial purposes; or made for commercial purposes, but does not include an advertisement or telemarketing.[39] Businesses that outsource their telemarketing or informational calls to third-party

[34] Id. ("Banks should implement effective compliance risk management systems, including processes and procedures to appropriately manage risks in connection with debt-sale arrangements. Examiners review banks' debt-sale arrangements for compliance with applicable consumer protection statutes and regulations. In particular, banks should ensure that all parties involved in the debt-sale arrangement have strong controls in place to ensure that sensitive customer information is appropriately protected."). Unfair, abusive or deceptive collection practices for small business loans may also bring scrutiny from the Federal Trade Commission and state regulators or attorneys general.
[35] 47 U.S.C. § 227.
[36] 16 C.F.R. part 310; 47 C.F.R. § 64.1200.
[37] 47 C.F.R. § 64.1200(a)(1)-(4); 47 C.F.R. § 64.1200(c); 47 C.F.R. § 64.1200(d).
[38] 47 C.F.R. § 64.1200(a)(1)(a)(2)(iii-iv); 47 C.F.R. § 64.1200(a)(2).
[39] 47 C.F.R. § 64.1200(a)(3).

service providers can still be held vicariously liable for TCPA violations on the basis of federal common law agency principles.[40]

- *The CAN-SPAM Act*

  The CAN-SPAM Act regulates the transmission of commercial e-mail messages. Commercial e-mail messages are defined as messages with a "primary purpose of . . . commercial advertisement or promotion of a commercial product or service," including emails to commercial addresses and to current or former customers.[41] The basic tenets of the CAN-SPAM Act are: not to use false or misleading header information; not to use deceptive subject lines; clearly identifying messages as ads; specifying the soliciting business' address; providing opt-out options for recipients and abiding by their requests; and monitoring what third parties are doing on your behalf. Companies using e-mail to market and advertise their products and services must have a compliance program in place, because the potential consequences for violations are high. Each separate email in violation of the CAN-SPAM Act is subject to penalties of up to $16,000.[42]

- *Telemarketer Sales (Do Not Call) Rule*

  The FTC's Telemarketer Sales Rule ("TSR") established the National Do Not Call Registry, where consumers can enter their numbers to reduce the telephone solicitations they receive. The law requires telemarketers to search the Registry every 31 days and avoid calling any phone numbers that are on the registry.[43] A telemarketer who disregards the National Do Not Call Registry could be fined up to $16,000 for each call.[44] Further, the TSR prohibits "credit card laundering," which it defines as presenting or depositing into the credit card system for payment a credit card sales draft generated by a telemarketing transaction that is not the result of a telemarketing credit card transaction between the cardholder and the merchant.[45]

- *Servicemember Civil Relief Act (SCRA) and Military Lending Act (MLA)*

  The SCRA protects active duty armed forces and active National Guard or Reserve duty members, along with their spouses and certain dependents, from high interest

---

[40] *In re Joint Petition Filed by DISH Network*, 28 F.C.C. Rcd. 6574 (2013).
[41] 15 U.S.C. § 7702(2)(A). The FTC has issued regulations implementing the CAN-SPAM Act. 16 C.F.R. Part 316. The FCC also has authority under the CAN-SPAM Act to issue rules addressing unsolicited commercial messages sent to consumers' wireless devices. *See generally* CAN-SPAM Act (Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003), Public Law 109-187; 15 USC 7701-7713**,** 18 USC 1001**,** 1037**;** 28 USC 994**; and** 47 USC 227**.**
[42] *The CAN-SPAM Act: A Compliance Guide for Business*, Federal Trade Commission, Sept. 2009, available at https://www.ftc.gov/system/files/documents/plain-language/bus61-can-spam-act-compliance-guide-business.pdf.
[43] 16 C.F.R. §310.4(b)(iii)(B).
[44] *Federal Civil Penalties Inflation Adjustment Act*, 74 Fed. Reg. 857 (Jan. 9, 2009) (to be codified at 16 C.F.R. § 1.98(d)) (increasing the maximum civil penalty from $11,000 to $16,000 per violation effective February 9, 2009).
[45] 16 C.F.R. §310.3(c).

loans. They are entitled to a number of financial protections, including a six percent cap on interest rates. Lenders cannot deny or revoke their credit, change the terms of an existing loan, or refuse to grant them credit because a service member sought SCRA protections; and civil court and administrative proceedings may be postponed.

New regulations under the Military Lending Act require lenders to implement policies to identify active duty service members, and forbid active duty servicemembers from obtaining loans with interest rates above 36%.[46] Online lenders, like their federally insured banking brethren, must take these responsibilities very seriously or face costly enforcement actions.

- *Fair Credit Reporting Act (FCRA)*

  The FCRA, [47] as amended by the Fair And Accurate Credit Transactions Act ("FACTA"), [48] regulates consumer reporting agencies, users of consumer reports and furnishers of consumer information to consumer reporting agencies. The law provides safeguards to limit when and how consumer report information may be used; requires consumer consent for most uses; provides for adverse action notices if the information leads to a denial of credit or other benefits; insures accurate credit reporting; and requires certain disclosures incident to a background check.

  Online lenders that may request consumer reports on prospective borrowers are "users" of consumer information and are subject to the FCRA's requirements. For institutions that lend to consumers, the FCRA governs underwriting and the type of data that can be used, as well as how and when a company must respond to a consumer dispute and accuracy requirements. Because many online lenders use underwriting sources that go beyond the traditional credit report, they often have additional FCRA responsibilities that traditional lenders may not face. Also, if an online lender reports to a consumer reporting agency any information related to a person's credit, the online lenders will be subject to the FCRA in its capacity as a furnisher of consumer information.

- *Truth In Lending Act (TILA)*

  TILA and its implementing Regulation Z govern the types of disclosures that lenders need to make to consumers. More specifically, TILA requires financial institutions to disclose virtually all extensions of consumer credit, which is defined as "credit offered

[46] 50 U.S.C. app. §§ 501 et seq.
[47] 15 U.S.C. 1§681 et seq.
[48] Pub. L. 108-159, 111 Stat. 1952.

or extended to a consumer primarily for personal, family, or household purposes."[49] TILA is a broad statute that covers a variety of open-end and closed-end loans, and the primary goal of the statute is to ensure credit terms are disclosed in a meaningful and clear way to consumers. TILA protects consumers from inaccurate and unfair credit card billing practices, provides rescission rights, establishes certain rate caps for dwelling-secured loans, imposes limitations on home equity lines of credit and prohibits unfair or deceptive mortgage lending practices.[50]
Each financial institution involved in an extension of credit, which includes transfers and payments, must comply with TILA and Regulation Z's disclosure requirements of consumer rights, finance charges and payment requirements.[51]

- *Ability-to-Pay Requirements*

  Certain types of consumer loans, such as credit card loans, require lenders to ascertain a consumer's ability to pay before a loan can be completed. Online lenders are subject to these requirements. For example, the Credit Card Accountability Responsibility and Disclosure Act of 2009 (CARD Act), which amended TILA, established new disclosure requirements instituting fair and transparent practices for open-end consumer credit plans. The Board of Governors of the Federal Reserve System issued similar rules shortly thereafter.[52] The new rules generally prohibit a card issuer from opening a credit card account or increasing a line of credit for any consumer unless it considers the consumer's ability to make the required payments under the terms of the account.[53] The regulations require that issuers consider the consumer's independent ability to pay, and impose additional consumer protective requirements for loans issued to consumers under the age of 21.[54] Similar rules were also developed in 2013 for assessing the consumer's ability to repay on a higher-priced mortgage loans.[55] The CFPB has also proposed extensive ability to pay requirements for short term loans in a recent rulemaking.

[49] 12 C.F.R. 1026.2(a)(12); *see also*, 12 C.F.R. Part 1026 Supplement I to 1026.2(a)(12).
[50] *CFPB Consumer Laws and Regulations: Truth in Lending Act* (June 2013) available at http://files.consumerfinance.gov/f/201306_cfpb_laws-and-regulations_tila-combined-june-2013.pdf
[51] 12 C.F.R. § 1025.5(a)(1)(ii)(B); see also § 1026.6, 1026.9.
[52] 12 C.F.R. § 226.51.
[53] 15 U.S.C. 1665e.
[54] 15 U.S.C. 1637(c)(8) (TILA section 127(c)(8)).
[55] 12 C.F.R. § 1026.

Payments Processing

A) New Payments Technology is More Secure and Convenient

Recent technological advancements have had a profound impact on the payments industry, providing consumers ever more convenient and secure means to pay for goods and services and enabling businesses to accept a variety of payment technologies while giving them almost instant access to the payments. Consumers can pay directly from mobile wallets using their smartphone at the touch of a single button. Merchants can handle transactions directly from a tablet or other mobile device, reducing lines at cash registers, speeding up commerce and giving them more payment options. Merchants participating in these programs receive payments in their accounts quickly, while consumers can check their credit card and bank account balances knowing that even transactions made a few seconds earlier are likely to be reflected. In addition, consumers' payment account information is protected with encryption and a variety of security measures and merchants can trust that customers are verified and authenticated through dozens of techniques. These improvements in convenience and security are available in brick and mortar commerce and the online and mobile commerce environments.

The network of hardware, software and service providers necessary to complete a payment is extensive. New payment companies design, manufacture, and program new systems that transmit payment information to the banks that issue the cards and the clearing house that moves payments from those banks to the merchants' accounts in other banks. Banks also provide deposit services to the processing companies, which maintain balances for all the merchants they work with to cover charge-backs due to customer disputes with the merchant. The payment processing industry also includes independent sales organizations ("ISOs"), which sign up merchants for the processors' networks.

This large ecosystem of payments providers is part of the vital financial infrastructure of the nation and, in fact, the world. For this reason, protection of the data that flows through the payments system is essential to the safe functioning of the economy. Due to its importance, the payments system provides a ripe target for theft, fraud, cyber-attack and other criminal activities. Because of these risks, companies and products in the payments system are heavily regulated, as detailed below.

To illustrate the regulatory process and requirements applicable to a new payments innovator, consider the hurdles that a hypothetical company trying to introduce a new product and service would face. Our entrant to the payments industry, which we will call "PayNow," has developed a new process to enable payments with a smartphone, using a new

combination of verification and security techniques, such as facial recognition or fingerprint. PayNow's technology and software would benefit consumers, merchants and issuing banks by reducing fraud, increasing consumer security, and accelerating commerce by providing a variety of convenient ways for consumers to pay merchants. PayNow will also increase convenience for customers by including a stored value feature on the card.

PayNow has invested heavily in research and development to innovate its technology, and has reached numerous agreements with banks and various other incumbent payment industry stakeholders. Having created a great product and received necessary permissions from other industry players, PayNow has to consider a number of regulatory requirements before it can get to market.

First, the processing technology must prove to regulators and dominant stakeholders that its system is secure. Even though PayNow has built a technology with security capabilities that far surpass industry rules, PayNow and its new product must comply with the PCI-DDS requirements, GLBA, Regulation P and the bank regulators' various Privacy Rules and informal guidance documents, as well as numerous state privacy and data security laws. In addition, PayNow needs to make sure it is in compliance with any additional data security requirements issued by the acquiring bank and the card brands it processes. PayNow's compliance department must have breach notification policies and procedures in place to comply with these laws and ensure that appropriate staff are well trained on them.

PayNow will need to study the FINCen anti-money laundering rules carefully to determine whether its stored value feature makes it subject to the customer due diligence and other requirements in those rules. The company must be certain that its Customer Identification Program ("CIP") is in compliance with the USA Patriot Act, to make sure that its devices are not used in the financing of terrorism. These laws include know-your-customer procedures and required systems to monitor transactions for suspicious behavior.

The stored value feature will also require the company to satisfy EFTA and Regulation E, requiring PayNow to provide appropriate notice and disclosures of terms and conditions to users of the product. Regulation E includes rules regarding reloading, restrictions on use, interest, finance, over-draft and other charges that may accrue, along with notices that alert users to the charges. PayNow will also need to review other federal and state consumer protection laws to make sure that its new device provides appropriate receipts and other required disclosures to consumers. Its compliance staff will need to analyze TILA, Regulation Z, card network rules and the FCRA to design its products so they avoid violations. The company must review the CFPB's "Nine Consumer Protection Principles" for Payment Processors and any subsequent guidance issued by that agency. State laws, regulations and licensing requirements must also be checked and complied with before merchants are approached. In addition, before accepting its first consumer payment, PayNow must be sure that its consumer consent procedures are compliant with federal and state E-SIGN statutes,

and that appropriate disclosures have been made when the consumer signed up for the card or other account or at the time of the transaction.

To the extent PayNow outsources any of its functions (which is common among specialized companies like PayNow which do not have the expertise and ability to carry out all of the applicable corporate, administrative, compliance and other requirements), it will need to make sure it has policies and procedures in place to on-board and supervise its service providers and monitor their compliance with applicable laws and regulations. This includes identifying any additional laws and regulations applicable to the service provider, educating itself on the appropriate level of compliance and auditing the service provider's policies, procedures and compliance metrics.

As a provider of a prepaid card, PayNow will have to conduct a detailed analysis of the money service business statutes, rules and license obligations in all 50 states, the District of Columbia and United States Territories to determine if it is a money service business and, if so, what type of license may be required.[56] Almost all the states have enacted the Uniform Money Services Act, the most recent version of which was published by the National Conference of Commissioners on Uniform State Laws in 2004.[57] However, the Uniform Act permits certain variations among the states, which also differ in their regulations, interpretations and enforcement policies under the Act.[58] PayNow's analysis could require conversations with the regulators in these various jurisdictions, to determine whether its product falls under the MSB requirements in each one.[59] The company compliance department will have to make sure the rules and regulations of those states are monitored and any changes incorporated into the company's policies and procedures. Similar to the lending licensing regime, the money transmitter license application process is different for every State and includes additional requirements and sometimes conflicting requirements that must be tracked by PayNow's compliance department.

Also on PayNow's list of regulatory compliance hurdles are the various AML/BSA and anti-terrorist financing statutes and regulations issued by the Treasury Department's Financial Crimes Enforcement Network ("FinCEN"). The company must make sure its onboarding process utilizes an adequate due diligence program for merchants (sometimes referred to as Customer Identification Program or CIP) to avoid those that raise unacceptable risks of

[56] The Uniform Act includes three categories of MSBs: Money transfer services, which can also engage in check cashing and currency exchange without having to obtain a separate license for that purpose; check cashing businesses, which can also engage in currency exchange (but not money transfers); and currency exchange services, which can only exchange currencies.
[57] Available on the Conference web site at http://www.uniformlaws.org/shared/docs/money%20services/umsa_final04.pdf.
[58] Differences include not only definitions, but, among other things, bonding requirements, net worth requirements and license fees.
[59] If PayNow did not offer a prepaid product, it might still be considered a MSB. Applicable statutory definitions are vague and depend upon the interpretation given them by state regulatory authorities. In most states, a payment processor currently is not considered to be a money transmitter, because it holds and transfers funds as an agent of the payee bank. Washington appears to be the lone exception. However, if the processor provides other services (e.g., gift cards, rewards programs) that cause it to create accounts or transfer value for consumers or other entities, even momentarily, it may be considered a money transmitter. State statutes and regulatory interpretations differ substantially on this issue and are in constant flux.

potential criminal enterprises. For merchants that have acceptable risks, it must employ controls to monitor transactions and, in particular, charge-backs to flag potential laundering, fraud and other illegal or abusive behavior. PayNow needs to be aware that it can be pursued by federal regulators as an accessory if it was in a position to detect this behavior and failed to do so. Regulators will bring enforcement actions directly or pressure Bank counterparties to prevent access to the banking system by a processor they deem complicit. To prevent processing payments to terrorists or nations that are subject to international sanctions, PayNow must fully understand the applicable regulations and frequently review the lists of terrorist and sanctioned entities published by the Treasury Department's Office of Foreign Assets Control or "OFAC."

Once it has set up and trained its compliance department on these and other laws and rules, and developed appropriate policies, procedures and controls, PayNow is almost ready to launch its new product. However, as with our hypothetical online lending product, the prudent approach is first to present the product to the various regulators, including the FTC, Federal Financial Institutions Examination Council ("FFIEC"), Federal Reserve, CFPB and other banking regulators to make sure they are familiar with it and do not react with skepticism or suspicion when it hits the market. (More mature companies that already have established bank partners and relationships are likely to work with their banks on setting up and implementing new products and services, including appropriate vetting with the regulators.) As previously discussed, these presentations also provide an opportunity to hear their concerns and to make any necessary adjustments to address them. Perhaps, most importantly, a bank will generally not utilize new technology services or products until it is certain that its regulators will not object.[60] The process of arranging the necessary meetings and waiting for feedback can take many months.

PayNow may also want to train its compliance staff and managers on what to expect in the regulatory audits and examinations, because, like any financial company, it most likely will be audited frequently and will be subject to examinations and investigations by various regulators. Specifically, while the CFPB and prudential bank regulators may not have direct supervisory authority, if the service provider has a relationship with a banking partner, these regulators for all practical purposes have authority to visit PayNow's facility and examine its books and records.[61] More frequently, its partner bank or banks will either audit PayNow or require it to obtain independent audits of its operations. All banks must do this to comply with guidance from their regulators, detailed below, governing relationships with technology providers and third party service providers. To newcomers to the financial industry, the presence of auditors and examiners must be included in any prudent business plan. The regulators and the bank partners will become familiar with the new technology and the new

[60] All payment processors work with bank partners, referred to as acquiring or payee banks, which hold funds for the processors' merchant customers.

[61] The term "prudential regulator" refers to the safety and federal safety and soundness regulatory agencies for federally insured depository institutions - the OCC, the FDIC, the Federal Reserve Board and the National Credit Union Administration.

vendor, while identifying any risks or weaknesses and making sure they are addressed quickly so as not to adversely affect the bank or any consumers.

B) Regulatory Requirements With Which a New Payments Service Must Comply

Like the online lenders discussed above, emerging payments companies face many of the same regulatory compliance challenges that banks face. As explained in the Introduction, to the extent there are differences in the regulatory regimes, it is because depository institutions (and SIFIs) create risks to the taxpayers or economy that payment processors do not. Nevertheless, the regulatory requirements faced by payment processors are extensive. A less than exhaustive list includes:

- *Gramm-Leach Bliley Act (GLBA), Privacy of Consumer Financial Information and Regulation P*

  GLBA and the CFPB's Regulation P require financial institutions to provide data security, breach notification and privacy and data sharing protections to consumers.[62] Payment Processors are considered "financial institutions" under the Privacy Rules, and are subject to these requirements, which are essentially the same as those detailed for online lenders above.

  However, Processors may not be directly subject to all of the Privacy Rules. For instance, Processors are not required to comply with the customer notice disclosure requirements prescribed by the FTC and CFPB Privacy Rules because consumers whose automated teller machines (ATMs), Point of service (POS), internet or telephone transactions are processed by processors do not become customers simply by effecting such transactions. A customer relationship is established when the consumer enters into a continuing relationship with the financial institution.[63] Processors are also exempt from these requirements because any nonpublic personal information shared in connection with a payment transaction is "necessary to effect, administer or enforce a transaction" requested by a consumer, or in connection with servicing or processing a financial product or service requested or authorized by a consumer.[64] Although processing payments does not create a customer relationship with the consumer under the applicable rules and does not, without more, give rise to notice requirements, if the processor also extends the credit, depository or other

[62] 15 U.S.C. § 6804.
[63] 16 C.F.R. 313.4(c), 12 C.F.R. 1016.4(c).
[64] 13 C.F.R. § 313.14(a)(1). The quoted phrase is further defined to mean, among other things: "In connection with the authorization, settlement, billing, processing, clearing, transferring, reconciling or collection of amounts charged, debited, or otherwise paid using a debit, credit or other payment card, check, or account number, or by other payment means." 13 C.F.R. § 313.14(b)(2)(vi)(A).

service to the consumer, it must also create a compliance function to ensure compliance with the Privacy Rules.[65]

- *GLBA and Customer Information Security Guidelines*

  Depending on the specific services they provide, payment processors are defined as "financial institution[s]," "service providers," or both and are subject to guidelines for safeguarding nonpublic personal information about customers that the FTC and the banking agencies have adopted to implement Sections 501 and 505(b)(2) of the GLBA (15 U.S.C. §§ 6801(b) and 6805(b)(2)).[66]

  Like all other financial institutions, as noted above in the Online Lenders section, the Guidelines require payment processors to develop and maintain comprehensive written information security programs; protect against any anticipated threats or hazards; and protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer.[67] Processor must also exercise appropriate due diligence in selecting service providers; contractually require service providers to implement appropriate security measures; and monitor the service provider's compliance with these obligations.[68] Again, as described in the Online Lending section, any security program must include a breach response program that will ensure proper incident response, communication to customers, third party compliance and law enforcement assistance.

- *GLBA and the FTC's Safeguards Rule*

  Payment processors fall within the broad definition of a business that is "significantly engaged" in providing financial products or services, and therefore are also financial institutions subject to the FTC's Standards for Safeguarding Customer Information ("Safeguards Rule"), codified at 16 C.F.R. Part 314. The Safeguards Rules is discussed in more detail in the Online Lending section above.

---

[65] Processors are not required to comply with the customer notice disclosure requirements prescribed by the FTC and CFPB Privacy Rules because consumers whose ATM, POS, internet or telephone transactions are processed by processors do not become customers simply by effecting such transactions. A customer relationship is established when the consumer enters into a continuing relationship with the financial institution. 16 C.F.R. 313.4(c), 12 C.F.R. 1016.4(c). Processors are also exempt from these requirements because any nonpublic personal information shared in connection with a payment transaction is "necessary to effect, administer or enforce a transaction" requested by a consumer, or in connection with servicing or processing a financial product or service requested or authorized by a consumer. 13 C.F.R. § 313.14(a)(1). The quoted phrase is further defined to mean, among other things: "In connection with the authorization, settlement, billing, processing, clearing, transferring, reconciling or collection of amounts charged, debited, or otherwise paid using a debit, credit or other payment card, check, or account number, or by other payment means." 13 C.F.R. § 313.14(b)(2)(vi)(A).

[66] *See supra* note 18.

[67] 12 U.S.C. § 3401(1); 16 C.F.R. § 314.3; 12 C.F.R. Part 364, Appendix B, Section II; 12 C.F.R. § Part 208, Appendix D-2, Section II. 12 C.F.R. Part 30, Appendix B, Section II; 12 C.F.R. Part 570, Appendix B, Section II.

[68] *See, e.g.*, 12 C.F.R. Parts 364 (Appendix B), 208 (Appendix D-2), 30 (Appendix B), 570 (Appendix B). *See also* Section III.D. of Appendix B to 12 C.F.R. Part 30.

- *Electronic Fund Transfer Act and Regulation E*[69]

  As noted in the Online Lenders section above, a primary focus of EFTA and Reg E is to ensure that customers who authorize electronic payments from their accounts receive proper disclosures.[70] Therefore, processors that operate debit or payment card systems or ATM networks must make sure that applicable disclosures, most of which relate to fees, can be made with their devices or at their terminals. Although a payment processor may not be subject directly to the EFT Laws, payments, transfers, ATM deposits/withdrawals and other EFTs processed by financial institutions through the processor are generally governed by, and must comply with, the EFT Laws.[71] Each financial institution or other person involved in an EFT, which includes transfers, payments and ATM transactions, is subject to the EFT Laws and, accordingly, must comply with the disclosure and other requirements prescribed by the EFT Laws.

  Here again, payment processors need to establish a substantial compliance program, to ensure compliance with EFTA and Regulation E.

- *Electronic Fund Transfer Act (Durbin Amendment) and Regulation II*

  The Durbin Amendment, which was enacted as part of the Dodd Frank Act, limits interchange fees and related compensation that may be charged by debit card issuers. It applies only to issuers with assets more than $10 billion.[72] Importantly, the regulations broadly define debit cards to include any code or device (other than paper checks or drafts or facsimiles thereof) issued or approved for use through a payment card network to debit an account.[73] They also include many general-use prepaid cards.[74]

  Further, Reg. II requires that an issuer must enable at least two unaffiliated payment card networks on each debit card.[75] It also prohibits an issuer or payment card

[69] 15 U.S.C. §§ 1693 et seq.; 12 C.F.R. Part 1005.
[70] Among other requirements prescribed by the EFT Laws, Regulation E requires financial institutions to make receipts available to a consumer at the time the consumer initiates an electronic fund transfer ("EFT") at an electronic terminal. 12 C.F.R. § 1005.9(a). Regulation E also requires disclosures of any ATM fees and prohibits charging the fees unless the consumer elects to continue the transaction or inquiry after receiving the disclosure. 12 C.F.R. 1005.16. For third party transfers, Regulation E requires that terminal receipts and periodic statements identify the name of the third party to or from whom funds are transferred. 12 C.F.R. 1005.9(a)(4), 1005.9(b)(1)(v).
[71] For purposes of Regulation E, an EFT includes "any transfer of funds that is initiated through an electronic terminal, telephone, computer, or magnetic tape for the purpose of ordering, instructing, or authorizing a financial institution to debit or credit an account;" and a financial institution means "a bank, savings association, credit union, or any other person that directly or indirectly holds an account belonging to a consumer, or that issues an access device and agrees with a consumer to provide [EFT] services." 12 C.F.R. 1005.2(i) and 1005.3(b); 15 U.S.C. §§ l693a(8) and 1693c(a).
[72] 12 C.F.R. 235.3-235.6; See also 12 C.F.R. Part 235, Appendix A, Sections 234.3-235.6.
[73] 12 C.F.R. 235.2(f); See also 12 C.F.R. Part 235, Appendix A, Section 235.2(f).
[74] 12 C.F.R. 235.5(c); See also 12 C.F.R. Part 235, Appendix A, Section 235.5(c).
[75] Id.

network from directly or indirectly inhibiting the ability of merchants to direct the routing of electronic debit transactions for processing over any payment card network of the merchant's choosing that may process such transactions.[76]

- *Bank Secrecy Act and Anti Money Laundering Regulations*

  The Bank Secrecy Act and its implementing regulations ("BSA Rules") are a mechanism by which the United States government combats drug trafficking, money laundering and other crimes.[77] The BSA Rules were enacted primarily to prevent banks and other financial service providers from being used as intermediaries for, or to hide the transfer or deposit of money derived from, such criminal activity.[78] They identify transactions and circumstances that must be reported to federal authorities. They also define compliance systems that must be employed.

  The function of processing payments does not fall directly under the BSA Rules, but to the extent that payment processors run credit card or certain types of prepaid account systems (gift cards, rewards cards and other stored value devices) they fall within the BSA Rules, just as any bank would. As such, they would also be subject to enforcement by the Treasury Department and the Justice Department. Payment processing companies must, therefore, maintain extensive compliance regimes to ensure that they are comply with the BSA rules and any requirements imposed by banks and card brands.

- *Other Know Your Customer's Customer ("KYCC") Actions*

  In recent years, various federal agencies have been using their examination authorities to persuade banks to drop customers or categories of customers deemed risky or undesirable.[79] These authorities can be used to cause banks to cut off deposit services to processors who are servicing merchants the regulators deem undesirable. This type of regulatory risk is similar to that faced by processors under the BSA/AML laws, where regulators require banks to scrutinize processors' on-boarding and monitoring programs to detect money laundering and terrorist financing, and is referred to

[76] 12 C.F.R. 235.7(b); See also 12 C.F.R. Part 235, Appendix A, Section 235.7(b).
[77] 31 U.S.C. § 5311-5330, 12 U.S.C. § 1829b, §§ 1951-1959; USA Patriot Act, 31 U.S.C. § 5312(a)(2) (expanding the AML program);, 31 C.F.R. Title X.
[78] *See, e.g.,* 31 U.S.C. §§ 5313(a) and 5318(g).
[79] For example, the FDIC was recently criticized by its Inspector General for utilizing this type of pressure tactics to eliminate tax refund loans. In its report, the Inspector General documented that senior management at the FDIC and OCC ignored the views of their own examiners that the loans did not threaten banks' safety and soundness and used threats and other tactics that were termed "moral suasion" to eliminate this form of lending. See, Federal Deposit Insurance Corporation Office of Inspector General, "Executive Summary - Report of Inquiry into the FDIC's Supervisory Approach to Refund Anticipation Loans and the Involvement of FDIC Leadership and Personnel," Report No. OIG-16-001 at 4 (Feb. 19, 2016) ("we believe more needs to be done to subject the use of moral suasion, and its equivalents, to meaningful scrutiny and oversight, and to create equitable remedies for institutions should they be subject to abusive treatment"); "Statement of Fred W. Gibson, Jr., Acting Inspector General, Federal Deposit Insurance Corporation" before the Committee on Financial Services, Subcommittee on Oversight and Investigations, U.S. House of Representatives (March 16, 2016). Both documents are available at https://www.fdicig.gov./.

generally as Know-Your-Customer's-Customer (KYCC) risk. The difficulty for processors is determining which merchants the regulators may find objectionable, because no written guidance is provided by the regulators.

- *Customer Identification Program Requirements (CIP Rules)*

  Section 326 of the USA PATRIOT Act directs the Secretary of the Treasury ("Secretary") to prescribe minimum standards requiring financial institutions to verify the identity of any person who seeks to open an account at the financial institution. The standards must include reasonable procedures for (i) verifying the identity of such persons, (ii) documenting the information used to verify the persons' identity, and (iii) consulting lists of known or suspected terrorists or terrorist organizations. The Secretary considers various types of accounts, methods of opening them and types of identifying information available. Several sets of regulations govern the different types of financial institutions, including 31 C.F.R. § 1020.220 governing banks. These requirements are pushed down by banks and other financial institutions to third party service providers (including payment processors) as required under various guidance documents issued by their regulators.

  Although not defined as "financial institutions," payment processors that run prepaid access programs (see definitions above) must comply with similar provisions.[80] Operators of credit card systems also have customer due diligence rules, which are pushed down to acquiring institutions, which include many processors.[81] As a result, most processors must establish compliance regimes to ensure compliance with these requirements.

- *State Money Transmitter Laws*

  Almost all states have their own money transmitter laws, designed to protect consumers, in addition to the federal remittance rules. Although payment processors do not deal directly with consumers, the states are divided on whether these laws apply to processors. Most have not yet made a determination. Guidance from Pennsylvania and Washington State indicate that they consider processors to be transmitters for purposes of state licensure laws and BSA.[82] New York, California, Texas and Illinois have followed the federal approach and concluded the opposite.[83]

---

[80] 31 C.F.R. § 1022.210(d)(1)(i).
[81] 31 C.F.R. § 1028.210.
[82] Pennsylvania Dept. of Banking, ltr. (Sept. 29, 2015), available at http://www.dobs.pa.gov/Documents/Secretary%20Letters/Money%20Transmitters/092915SecretaryLetterMoneyTransmission.pdf ; State of Washington, Dept. of Fin. Svcs., Div. of Consumer Svcs., Interpretive Stmt. 2016-1 (Dec. 7, 2015), available at http://www.dfi.wa.gov/sites/default/files/opinions/mt-2016-01.pdf .
[83] New York Dept. of Fin. Svcs., Banking Interpretation 640 (Nov. 18, 2004), available at: http://www.dfs.ny.gov/legal/interpret/lo041118.htm; Cal Fin Code § 2010 (l); 7 Tex Admin Code § 33.4(a); Illinois Interpretive Guidance

However, some of the larger processors are also in the online money transmission business and must comply with money transmission laws in all the states.

As with other areas where state laws are not uniform, such as escheatment, or they are layered on top of the federal rules, it is a challenge for companies' compliance departments to comply with their sometimes conflicting, ambiguous, or redundant requirements. Processors must maintain an elaborate compliance program to deal with them.

- *State Escheatment Laws*

  Escheatment is the process of identifying a person's accounts that are considered abandoned, and remitting those funds to the state. State escheatment laws vary widely in terms of timing, what process must be undertaken to contact an account holder or successor in interest, and under what circumstances an account is considered abandoned. Because processors control accounts for merchants they service, compliance with these myriad laws is an important issue.

- *Federal Deposit Insurance Corporation Supervisory Guidance*

  A non-depository processor is not directly subject to the FDIC's guidance documents, but risks having its depository and other services with banks terminated if the standard articulated in the guidance deems the processor's services to be high risk. The practical effect of such termination would be to put the processor out of business. Specifically, FDIC's *Financial Institution Letters* ("FILs") and *Supervisory Insights* publications regarding payment processor relationships with depository institutions provide an overview of the primary risk areas on which examiners and financial institutions' audit teams will review any new processing service.[84]

  A processor's compliance department must remain up-to-date on the FDIC's guidance and make sure that internal policies and procedures are in place to provide satisfactory assurance that the guidance is followed.

- *Federal Financial Institutions Examination Council (FFIEC) Guidance and Examination*

("Statement Regarding Third-Party Payment Processors and the Transmitters of Money Act"), available at: http://idfpr.com/DFI/CCD/pdfs/07292015StatementThirdPartyProcTOMA.pdf.

[84] *FDIC Clarifying Supervisory Approach to Institutions Establishing Account Relationships with Third-Party Payment Processors*, Financial Institution Letter, FDIC, FIL-41-2014 (July 28, 2014), https://www.fdic.gov/news/news/financial/2014/fil14041.pdf; *FDIC Supervisory Approach to Payment Processing Relationships With Merchant Customers That Engage in Higher-Risk Activities (Rev. July 2014*), Financial Institution Letter, FDIC, FIL-43-2013 (Sept. 27, 2013) https://www.fdic.gov/news/news/financial/2013/fil13043.pdf; *Guidance on Payment Processor Relationships* (Rev. July 2014), Financial Institution Letter, FDIC, FIL-127-2008 (Nov.7, 2008), https://www.fdic.gov/news/news/financial/2008/fil08127.pdf; *see also Managing Risks in Third-Party Payment Processor Relationships (Rev. July 2014)*, Supervisory Insights, FDIC (Summer 2011), https://www.fdic.gov/regulations/examinations/supervisory/insights/sisum11/managing.html.

The examination authorities of federal banking regulatory agencies,[85] which comprise the FFIEC,[86] include regulating and examining services provided to insured depository institutions by third parties, such as payments processors.[87] Because payment processors typically must contract with a sponsoring bank or banks to process payments, they are considered IT service providers subject to examination by the FFIEC members.[88] The FFIEC provides guidance to financial institutions regarding considerations that depository financial institutions must take into account in third party relationships, such as data security, availability and integrity of systems and compliance.[89] As service providers to banks, payments companies must comply with the Council's guidance, are subject to examination by all the prudential bank regulators (state and federal) and the CFPB, and subject to audit by all their depository financial institution counterparties.

To help ensure compliance and deal with the examinations and audit requests, payment companies must maintain detailed compliance policy manuals and compliance programs and controls. A chief compliance officer is required at a minimum, generally full time, and other staff depending on the types of payments businesses and the states in which the company operates.

- *Telephone Consumer Protection Act*

  Payment processors whose business models include marketing payment or credit devices to consumers must be aware of and comply with the Telephone Consumer Protection Act, which is discussed in more detail in the Online Lending section above.

- *Telemarketer Sales (Do Not Call) Rule*

---

[85] 12 U.S.C. §§ 1248(a), 1463(a)(1), 1756 and 1819(a).
[86] Financial Institutions Regulatory and Interest Rate Control Act (FIRA), Title X, Pub. L. 95-630, 92 Stat. 3641 (1978) (codified as amended in scatter section of 12 U.S.C.).
[87] OCC Bulletin 2013-29 (Risk Management Guidance on Third-Party Relationships), available at http://www.occ.gov/news-issuances/bulletins/2013/bulletin-2013-29.html.
[88] The FFIEC's *Retail Payment Systems Examination Handbook* (2010) provides comprehensive guidance to examiners on risks to depository financial institutions that provide payment processing services, as well as a step by step guide to preparing for an examination or audit of compliance with customer due diligence regulations and with other expectations of federal regulators. It is available at: http://ithandbook.ffiec.gov/ITBooklets/FFIEC_ITBooklet_RetailPaymentSystems.pdf.
[89] FFIEC publishes on its website an extensive *Information Technology Examination Handbook* for use in connection with such examinations. Categories of the Handbook with particular applicability to payment processors include *Retail Payment Systems* (highlighted *supra*, n. 37); *E-Banking* (Aug. 2013), available at http://ithandbook.ffiec.gov/ITBooklets/FFIEC_ITBooklet_E-Banking.pdf; *Information Security* (July 2006), available at http://ithandbook.ffiec.gov/ITBooklets/FFIEC_ITBooklet_InformationSecurity.pdf; *Supervision of Technology Service Providers* (Oct. 2012), available at http://ithandbook.ffiec.gov/ITBooklets/FFIEC_ITBooklet_SupervisionofTechnologyServiceProviders(TSP).pdf; *Outsourcing Technology Services* (June 2004), available at http://ithandbook.ffiec.gov/ITBooklets/FFIEC_ITBooklet_OutsourcingTechnologyServices.pdf; *Business Continuity* (Feb. 2015), available at http://ithandbook.ffiec.gov/ITBooklets/FFIEC_ITBooklet_BusinessContinuityPlanning.pdf; and *Audit* (April 2012), available at http://ithandbook.ffiec.gov/ITBooklets/FFIEC_ITBooklet_Audit.pdf.

The FTC's Telemarketer Sales Rule ("TSR") is discussed in the Online Lending section above, because it has direct application to consumer-facing businesses. Recently, the FTC has used the TSR as a means of imposing liability on payment processors who provided processing services to telemarketers that violated the TSR, alleging they provided "substantial assistance" to the telemarketers.[90] For this reason, processors must establish and maintain merchant "due diligence" programs to help them avoid processing payments for any party that might be accused of violating this rule.

- *Unfair and Deceptive Acts and Practices ("UDAP") under the Federal Trade Commission Act*

  The Federal Trade Commission Act ("FTC Act") endows the FTC with significant investigative and enforcement powers. Relevant for payment processors, Section 5 of the FTC Act (15 U.S.C. § 45) empowers the FTC to prohibit unfair or deceptive trade practices. As discussed in the Safeguards Rule section, above, payment processors are financial institutions subject to the FTC's jurisdiction and may be subject to enforcement actions by the FTC if the FTC believes they have engaged in any unfair or deceptive trade practices or anti-competitive practices. The FTC does not have authority to issue regulations defining what it considers UDAP to be, but instead publicizes the enforcement actions it brings under this provision to provide guidance.

  Processors' compliance programs must monitor their business practices and all the FTC's enforcement actions to help ensure that the companies do not engage in activities or programs that could be considered UDAP.

- *Unfair, Deceptive and Abusive Acts and Practices ("UDAAP") under the Dodd Frank Act*

  Under the Dodd Frank Act, payment processors, like financial institutions, are subject to enforcement for alleged UDAAP violations. The CFPB has not yet issued regulations defining UDAAP for payment processors, although it has published *Consumer Protection Principles* for the industry, discussed below. A recent decision from the Northern District of Georgia has held that payment processors are "service providers" within the meaning of the Act.[91]

- *CFPB's "Nine Consumer Protection Principles" for Payment Processors*

  On July 9, 2015, CFPB released on its website a list of nine principles that describe the agency's vision for protecting consumers.[92] However, the CFPB has given no guidance

[90] *Federal Trade Commission v. Capital Payments, LLC*, No. 16-CV-00526-ADS-AYS, Stipulated Order for Permanent Injunction and Monetary Judgment at 2 (E.D.N.Y., Feb. 3, 2016), available at https://www.ftc.gov/system/files/documents/cases/160211bluefinorder.pdf.
[91] *CFPB v. Universal Debt & Payment Solutions, LLC*, Civil Action No. 1:15-CV-00859-RWS (N.D. Ga. Sep. 1, 2015).
[92] http://files.consumerfinance.gov/f/201507_cfpb_consumer-protection-principles.pdf.

on how, specifically, these principles are to be implemented. Too voluminous to restate fully here, the titles to the nine principles are:

1. Consumer control over payments
2. Data and privacy
3. Fraud error and resolution protections
4. Transparency
5. Cost
6. Access
7. Funds Availability
8. Security and payment credential value
9. Strong accountability mechanisms that effectively curtail system misuse

Payment processors' compliance departments must analyze this guidance and monitor litigation and enforcement actions constantly to mitigate risks that they will be accused of UDAAP or other violations that have not been fully articulated by the agencies or the courts

- *Remittance Transfer Rule*

  Certain larger payment processors are subject to the CFPB's remittance transfer rule because they process a large number of international money transfers. The rule amended Regulation E regarding remittances - money wired abroad to consumers or businesses - to require companies that make those services available to provide additional protections to consumers.[93] Those provisions include disclosure requirements and provisions for error resolution and cancellation.

  The rule requires companies that provide remittance services to train staff on new policies and procedures and adopt new forms and disclosures, which may require legal review. It adds another area for which the companies must develop controls and that the compliance department must continually monitor for updates and changes.

- *Card Association and Network Rules*

[93] *Report of Inquiry into the FDIC's Supervisory Approach to Refund Anticipation Loans and the Involvement of FDIC Leadership and Personnel*, Federal Deposit Insurance Corporation, Office of Inspector General, Report No. OIG-16-001 (February 19, 2016)

The credit card networks, as well as the ATM networks, have voluminous operating rules that impose numerous requirements on payment processors. The most notable of these is the National Automated Clearing House Association ("NACHA"). NACHA manages the ACH Network, the backbone for the electronic movement of money and data in the United States. Payment processors are subject to the NACHA Operating Rules, a highly detailed set of rules that guide risk management and create certainty for all participants.[94]

- *PCI Compliance Data Security Standards*

  The Payment Card Industry Data Security Standard (PCI DSS) is a set of requirements, published by the PCI Security Standards Council ("Standards Council") on its website, designed to ensure that all companies that process, store or transmit credit card information maintain a secure environment. The Standards Council is comprised of the five major credit card brands and other "Strategic Members" from the payments industry. The PCI DSS, which are recognized internationally as the governing industry standards for the payments industry, are extraordinarily detailed and updated frequently by the Standards Council to deal with new threats and other developments. The standards apply to any organization or merchant, regardless of size or number of transactions, that accepts, transmits or stores any cardholder data. All payment processing companies must comply with these standards and all are audited and examined against them.

- *Fair Credit Reporting Act*

  The FCRA contains a receipt "truncation" requirement that requires that a person who accepts credit or debit cards may not print more than the last five digits of the card number, or print the expiration date, on any electronically printed receipt given to a cardholder at the point of the sale or transaction.[95]

- *Unlawful Internet Gambling Enforcement Act*

  The Unlawful Internet Gambling Enforcement Act ("UIGEA") prohibits gambling businesses from knowingly accepting payment (e.g., credit, electronic fund transfers, check or draft and proceeds from any form of a financial transaction) in connection with the participation of another person in a bet or wager that involves the use of the internet and that is unlawful under any federal or state law in the Act. [96] UIGEA's accompanying regulations further require that certain "participants" in payment systems that could be used for unlawful internet gambling to have policies and procedures reasonably designed to identify and block or otherwise prevent or

[94] Available by subscription for NACHA members on the NACHA website.
[95] 15 USC 1681c(g).
[96] 31 U.S.C. § 5163.

prohibit the processing of restricted transactions.[97] A "participant" is "an operator of a designated payment system, a financial transaction provider that is a member of or, has contracted for financial transaction services with, or is otherwise participating in, a designated payment system, or a third-party processor."[98]

Unless their systems fall within certain narrow exceptions, payment processors must "establish and implement written policies and procedures reasonably designed to identify and block or otherwise prevent or prohibit restricted transactions."[99] They must also identify and block restricted transactions; or otherwise prevent or prohibit the acceptance of the products or services of the designated payment system or participant in connection with restricted transactions, in accordance with their policies and procedures.[100]

[97] 31 U.S.C. § 5163
[98] 12 C.F.R. § 233.2(w) (Regulation GG).
[99] 31 C.F.R. § 132.5(a); 12 C.F.R. § 233.5(a).
[100] 31 C.F.R. § 132.5(b)(1)(i)-(ii); 12 C.F.R. § 233.5(b)(1)(i)-(ii).

Data Security Regulation of Financial Technology

Data security laws and regulations have been outlined in detail in the preceding sections, but it is helpful to address in more detail the data security regime that governs the operations of any financial technology company that is involved in lending or payment processing. In this discussion, there are two important points to keep in mind. First, there is no evidence that data breaches and hacking that might occur in the online lending and payments processing industries would be prevented by more financial regulator examinations of lenders or processors. Second, the criminals and rogue nations who perpetrate these attacks are often highly sophisticated and able to adapt quickly to countermeasures. To adapt to the ever-changing data security challenges, companies must have the flexibility to move as fast as the criminals. They must be free to develop and deploy new systems and technology to protect their customers' data.

A) Primary Federal Data Security Regulators: FTC and CFPB

Currently lenders and processors are both regulated directly by the FTC and by the states in which they do business. Although the FTC does not have "examination" or "visitation" authority like bank regulators, it can accomplish much the same thing if it perceives a company as creating a risk to privacy by issuing a civil investigative demand, known as a "CID." This tool can be used in the same manner as an examination to gain access to all relevant documentation at a company and obtain testimony from employees. The FTC's UDAP authority, in particular, empowers the FTC to investigate the adequacy of data security.[101] The state regulatory agencies often have both examination and enforcement powers, and state attorneys general can use subpoenas to investigate suspected criminal actions that involve lenders or processors.

The CFPB directly regulates financial technology companies that lend to consumers and is taking action against payment processors, for which it has already issued regulatory guidance, discussed above. However, the CFPB also has authority to examine processors and lenders because they are service providers to banks and they handle consumer data. For these reasons, the CFPB has authority to examine online lenders and processors whenever it deems them to pose a threat to consumers.[102] Like the FTC, the CFPB also has its own UDAAP authority and a full range of enforcement powers available, and it can issue CIDs, cease and desist orders and civil money penalties to investigate and remedy deficiencies it

[101] See, cases listed on FTC web site at https://www.ftc.gov/datasecurity.
[102] 12 U.S.C. § 5536, 5561-5564.

suspects in data security.[103] In the *Dwolla* case, referred to in note 109, the CFPB recently used its UDAAP authority to fine a new financial technology company for simply mischaracterizing its security practices, even though no breach or other harm came to consumers.

B) Prudential Bank Regulators' Data Security Examination Flow-Down

In addition to the FTC and CFPB, most or all financial technology lenders and processors are subject to examination by the prudential bank regulators OCC, the FDIC, the Federal Reserve banks, the National Credit Union Administration and state financial institution regulatory agencies. These regulators define new technology entrants that work with banks as "service providers" to the banks.[104] As described above, it is very challenging for an online lender to compete without partnering with a bank. Likewise, all independent payments processors contract with acquiring banks to process payments from merchants into the banks' payment networks.[105] Thus, any new technology entrant that partners with a financial institution also will invite prudential regulators to examine its data security practices.

Regulators generally target resources at banks and other large financial institutions that lend and process payments. This strategy makes sense if only because these large financial institutions have been the target of some the largest data breaches in history.[106] Equally importantly, however, these financial institutions can be viewed as hubs through which all payments information must pass. That does not mean that breaches cannot occur elsewhere in the payment ecosystem, but the banks manage and operate existing payment networks, and prudential regulators hold the banks responsible for monitoring and enforcing the rules in their payment networks. In turn, the security systems of processors and lending partners are heavily audited as a flow-down consequence this prudential oversight. For example, the OCC requires that in any contract with a service provider the bank must:

> ensure that the contract establishes the bank's right to audit, monitor performance, and require remediation when issues are identified. Generally, a third-party contract should include provision for periodic independent internal or external audits of the third party, and relevant subcontractors, at intervals and scopes consistent with the bank's in-house functions to monitor performance with the contract. A bank should include in the contract the types and frequency of audit reports the bank is entitled to receive from the third party (e.g., financial, SSAE 16, SOC 1, SOC 2 and SOC 3 reports, and security

[103] 12 U.S.C. §§ 5561-5564; 12 C.F.R. part 1080 (rules for investigations); 12 C.F.R. part 1081 (rules for adjudication of enforcement actions).
[104] Supra, n. 4.
[105] Some card brands, such as American Express and Diners Club do not use third party processors.
[106] *See*, *e.g.*, "Prosecutors Announce More Charges in Hacking of JPMorgan Chase," New York Times (Nov. 10, 2015) (Over 85 million customer records hacked from J.P. Morgan Chase Bank in largest hacking scheme ever prosecuted), available at http://www.nytimes.com/2015/11/11/business/dealbook/prosecutors-announce-more-charges-in-jpmorgan-cyberattack.html?_r=0.

> reviews). Consider whether to accept audits conducted by the third party's internal or external auditors. Reserve the bank's right to conduct its own audits of the third party's activities or to engage an independent party to perform such audits. Audit reports should include a review of the third party's risk management and internal control environment as it relates to the activities involved and of the third party's information security program and disaster recovery and business continuity plans.[107]

The bank is specifically directed to use these audit powers to "ensure" compliance by the service provider with "certain provisions of the Gramm-Leach-Bliley Act (GLBA) (including privacy and safeguarding of customer information)."[108] The regulators thus marshal their resources and step in to examine or investigate the service providers when they suspect that the banks have not been doing their job. Because these examinations and investigations are confidential, they generally only come to light when the agency sues or brings an enforcement action, as in the recent cases against Dwolla and Integrity Advance.[109]

C) Marketplace Mandates, Audits and Reputation

Processors, like all other participants in payment card systems, are also audited against the PCI-DDS, standards that the payments industry maintains to guard against security breaches. Any payments company that does not comply risks being cut off by MasterCard or Visa, which is tantamount to putting the company out of business.

Suggestions that this extensive examination and auditing regime are inadequate are misplaced. Few, if any businesses are more closely scrutinized for the adequacy of their data security than new technology companies engaged in payments or lending. In fact, the primary areas where regulators worry about financial technology - the security and protection of digitized data - are the very areas in which newer technology companies have demonstrated the expertise to innovate most effectively.

New technology entrants generally have no business *other* than their digital business, and any loss of consumer trust in their data security practices could be crippling. New technology entrants have strong incentives to employ exceptional data security practices. They are much more likely to build a modern technology infrastructure and adopt the cutting edge security practices of the broader technology community, which has an excellent track record when it

[107] OCC Bulletin 2013-29 at 8.
[108] Id.
[109] *In the Matter of Dwolla, Inc.*, Administrative Proceeding File No. 2016-CFPB-0007, Consent Order (Feb. 27, 2016) available at http://files.consumerfinance.gov/f/201603_cfpb_consent-order-dwolla-inc.pdf and *In the Matter of Integrity Advance, LLC, et. al.,* Administrative Proceeding File No. 2015-CFPB-0029 (Nov. 18, 2015) see: http://www.consumerfinance.gov/about-us/newsroom/cfpb-takes-action-against-online-lender-for-deceiving-borrowers/

comes to handling consumer privacy and security - and has largely avoided the most serious data breaches in recent years.[110]

In summary, new technology entrants providing lending or payment services have an exhaustive set of reasons to protect security: FTC investigators, CFPB examiners, state examiners, bank auditors, card brand audits, the looming threat of private litigation and the disastrous negative publicity. However, despite that extensive government oversight and marketplace incentives to invest in security, data breaches still may happen, and no company, or sector, should claim perfection.

D) Modern Security Technology Benefits New Technology Entrants [and Banks Alike]

As security threats have become more sophisticated and ubiquitous, technology companies have worked tirelessly to ensure they are sufficiently nimble and able to respond quickly to and neutralize new kinds of threats. Technology companies have also been the first to develop and adopt new and superior security practices, such as tokenization of payment data, end-to-end encryption of data, two-factor authentication, mobile device ID and geolocation and biometric authentication. New financial technology entrants offering lending services or payment services are among the very companies that are working to identify and stave off cyber threats and adopt or engineer stronger security technologies. They are doing so because the marketplace is driving better fraud prevention and consumer protection, often times exceeding what may be required by regulators. And, while anecdotal breaches will always occur at technology companies just as at other businesses, for the reasons highlighted above, they pale into insignificance compared to the breaches at banks and major retailers.

Unfortunately, some traditional financial stakeholders suggest that more bank-like prudential examinations will somehow solve security challenges. Again, the evidence would indicate the opposite is true. Not surprisingly, according to a leading annual cybersecurity study conducted by Verizon, government and the technology, media and telecom sectors *combined* accounted for only 8.6% of all data breaches 2015. In contrast, prudentially regulated financial institutions, which experienced only 33 % more attacks than the technology industry, had the largest share of breaches of any sector at 35%.[111] Many of these incidents represent large-scale, systemic attacks that involve the loss of personal information of millions of Americans, or in some very recent incidents, the theft of tens of millions of

---

[110] *See* Bill Hardekopf, *The Big Data Breaches of 2014*, FORBES (Jan. 13, 2015), http://www.forbes.com/sites/moneybuilder/2015/01/13/the-big-data-breaches-of-2014/#309d083f3a48; *see also* Lorenzo Ligato, *The 9 Biggest Data Breaches of All Time*, HUFFPOST TECH (Aug. 20, 2015), http://www.huffingtonpost.com/entry/biggest-worst-data-breaches-hacks_us_55d4b5a5e4b07addcb44fd9e.

[111] *2016 Data Breach Investigation Report* at 3-5 (conducted by Verizon with contributions from 70 other companies), available at http://www.verizonenterprise.com/DBIR/2016/.

dollars from bank payment systems.[112] Federal financial regulators themselves have been victims of numerous cyberattacks,[113] causing some to worry about a loss of public confidence in these regulators' cybersecurity systems.[114] Certainly, there is no evidence that federal prudential regulators have prevented data breaches at the banks they regulate, with such breaches almost tripling in just one year, from 2014 to 2015.[115]

Rather than entrusting government bank examiners with data security, federal policymakers should work to ensure that any regulation, prudential or otherwise, enables modern data security through a principles-based approach that ensures technology-neutrality. Such an approach should apply to both financial institutions and new technology entrants, freeing both to focus on the best technology, not simply passing the next examination. The greater risk is that well-meaning regulators may impose overly rigid standards or best practices that are designed to prevent the last breach, rather than the next one.

[112] *See* Tom Bergin and Nathan Layne, *Special Report: Cyber Thieves Exploit Banks' Faith in SWIFT Transfer Network*, Reuters (May 20, 2016), http://www.reuters.com/article/us-cyber-heist-swift-specialreport-idUSKCN0YB0DD

[113] *See* Jason Lange and Dustin Volz, *Fed Records Show Dozens of Cybersecurity Breaches*, Reuters (June 1, 2016), http://www.reuters.com/article/us-usa-fed-cyber-idUSKCN0YN4AM; *see also* Joe Davidson, *FDIC Reports Five 'Major Incidents' of Cybersecurity Breaches Since Fall*, The Washington Post (May 9, 2016), https://www.washingtonpost.com/news/powerpost/wp/2016/05/09/fdic-reports-five-major-incidents-of-cybersecurity-breaches-since-fall/?tid=a_inl.

[114] *See* Joe Davidson, *FDIC Cyberattacks Included Hit on Former Chairwoman's Computer*, The Washington Post (May 11, 2016), https://www.washingtonpost.com/news/powerpost/wp/2016/05/11/fdic-cyberattacks-included-hit-on-former-chairmans-computer/.

[115] *Supra*, n. 106; 2015 *Data Breach Investigation Report* at 3, available at http://www.verizonenterprise.com/DBIR/2015/;

Conclusion

Online lenders and new payment processors are bringing important innovations to the financial market. Their new ideas help drive value and efficiency for consumers and small businesses.

Like banks, these companies are heavily regulated within their respective business lines. They are, in fact, subject to the same regulations as banks and are subject to extensive oversight by government agencies, bank customers, card brands and their insurance companies. For any new entrant, these regulatory burdens constitute a significant barrier to entry that require millions in compliance costs, staffing and significant delays in time to market.

If anything, the regulatory playing field is heavily tilted against new entrants. Nonetheless, innovators are dealing with these compliance burdens wherever necessary, and new technologies are helping consumers and small businesses by making financial services more accessible, affordable and secure.