Payment Systems: Regulatory Interest in Payment Processors, Faster Payments, and Related Consumer Protections

Executive Summary

The expansion of the Internet and the growth in electronic payments has significantly increased consumer demand for a variety of payment options and faster payments. The increased number of available electronic payment options and the volume of activity have heightened financial services regulators' interest in payment processors and the potential risks they may pose to financial institutions (as both account customers and service providers) and to consumers (because of their role in the infrastructure through which consumer make payments to merchants). Most recently, the regulators have placed additional scrutiny on the processes and activities performed by payment processors and have focused regulatory guidance on the need for related parties to engage in risk assessments, due diligence, and ongoing relationship monitoring. In particular, the guidance indicates that financial institutions that directly or indirectly provide payment processing for merchant customers are expected to assure themselves the merchant customers are operating in accordance with applicable laws and that they (financial institutions) are not facilitating fraudulent or other illegal activity. Similarly, the Consumer Financial Protection Bureau ("CFPB" or "Bureau") expects the bank and nonbank providers of consumer financial products and services under its authority and their service providers, including payment processors, to comply with the federal consumer financial laws as well as to assure themselves that their merchant customers are also operating in accordance with those laws.

The demand for faster payments, and push toward real-time payments, is being fueled by rapid technological innovations that impact elements supporting the payment process. In the U.S., both the Federal Reserve Board ("Federal Reserve") and the National Automated Clearing House Association ("NACHA") have announced "faster payments" initiatives and payment stakeholders, such as payment processors, have begun work to develop faster payment systems. This month, the CFPB published an outline of nine Consumer Protection Principles ("Principles") that the Bureau would like to be considered and incorporated into the architecture of the new payment systems under development in the United States. The CFPB notes that there is "substantial opportunity to improve efficiency, reduce transaction costs for participants, and reduce credit and fraud risks" throughout U.S. payment systems and it supports industry efforts to develop faster and safer consumer payment capabilities.

Background

Changes in the payment process brought about by new technologies and innovations effect changes in the nature of commerce and end-user expectations for payment services. Gaps and fragmentation have begun to develop in the U.S. and abroad between traditional payment services that operate on the older infrastructures and emerging services and service providers that are meeting increasingly demanding market expectations with new product offerings (e.g., mobile wallets). Payment stakeholders in the U.S., including the Federal Reserve, NACHA, and private industry participants (e.g., companies in the technology and finance fields), have been independently initiating actions to improve the "end-to-end" payment speed and security with the ultimate goal of reaching real-time payment systems.

Speaking before The Clearing House (one of two operators in the automated clearing house (ACH)) in November 2014, CFPB Director Richard Cordray acknowledged the change and growth in the industry, noting that the ACH network had processed nearly 22 billion ACH transactions in 2013, representing a 5 percent increase over the previous year. He outlined the CFPB's concerns with regard to electronic payment networks, which he defined to include "the ACH system, debit card networks and the

emerging domain of faster payments," listing among them the possibility for misuse / abuse and consumer harm (e.g., unauthorized transactions, repeated collection attempts, and cyber threats), issues surrounding funds availability (e.g., differences in the timing of funds being cleared and becoming available, and faster access), and costs associated with debit transaction ordering. With regard to faster payments in particular, he stated that a faster payment system could bring greater transparency and less need for individuals to "go outside the system to obtain access to their funds and to pay their bills," which would be "important advances for consumers."[1]

Director Cordray expressed support for the development of faster payment systems and even real-time payment systems, admonishing participants to "move as quickly as you can." He added, "…as you go about this work, it is essential that the interest of consumers remain at the top of your minds. After all, the objective here is to maintain an effective payment system for the sake of your customers."

"Faster Payments Initiatives"

The Federal Reserve published a multi-faceted plan for collaborating with payment system stakeholders to create a "safer, more efficient, and faster payment system" in January 2015. Entitled "*Strategies for Improving the U.S. Payment System*," the plan reflects strategies with "broad payment stakeholder support," including large and small businesses, emerging payments firms, card networks, payment processors, consumers, and financial institutions. The Federal Reserve identifies the following strategies as ones that would improve the U.S. payment system:

- Actively engage with stakeholders on initiatives designed to improve the U.S. payment system (to include the establishment of a faster payments task force and a payment security task force);
- Identify effective approaches for implementing a safe, ubiquitous, faster payments capability in the U.S. (beginning 2015);
- Work to reduce fraud risk and advance the safety, security and resiliency of the payment system (beginning 2015);
- Achieve greater end-to-end efficiency for domestic and cross-border payments (to include work on standards, directories, and business-to-business payment improvements - 2015 and beyond); and
- Enhance Federal Reserve Bank payments, settlement and risk management services (to include promoting greater use of same-day ACH capabilities - 2015 and beyond).

In May 2015, NACHA announced the approval of a final rule[2] that amends it Operating Rules to enable an ACH Originator the option to send same-day ACH transactions to any receiving financial institution ("RDFI"). The same-day option is available for both credit and debit transactions, though international transactions and transactions in excess of $25,000 are ineligible. The new capabilities will become available on a phased-in basis beginning September 2016 for credit transactions, September 2017 for debit transactions, and March 2018 for RDFIs to provide funds availability for same-day credit entries. NACHA states that effective dates of the three implementation phases are contingent on receiving written confirmation from the Federal Reserve to support the rule, which it adds is necessary to ensure that same day ACH is "ubiquitous across all 12,000 financial institutions in the U.S."

Regulatory protections are provided to consumers making and receiving ACH payments through a number of laws and regulations, including, among others, the:

- *Electronic Funds Transfer Act* ("EFTA") and its implementing regulation, Regulation E;
- *Truth-in-Lending Act* ("TILA") and its implementing regulation, Regulation Z;
- *Consumer Financial Protection Act* ("CFPA") prohibitions against unfair, deceptive, or abusive acts or practices ("UDAAP");
- *Federal Trade Commission Act* ("FTC Act") prohibitions against unfair or deceptive acts or practices ("UDAP");
- *Bank Secrecy Act*;
- *USA PATRIOT Act* (including its Know Your Customer provisions);
- *Foreign Corrupt Practices Act;* and
- NACHA Operating Rules.

[1] http://www.consumerfinance.gov/newsroom/prepared-remarks-of-cfpb-director-richard-cordray-at-the-clearing-house/

[2] https://www.nacha.org/news/nacha-membership-approves-same-day-ach

CFPB's Consumer Protection Principles for Faster Payment Systems

The Bureau suggests that features embodying the following Principles should be incorporated into the development of faster payment systems to increase the probability that they are safe, transparent, accessible, and efficient for consumers.

Consumer Control Over Payments - Payments should align with consumer authorizations (e.g., when, how), consumers should be able to set parameters that limit payments, and consumers should be able to easily revoke an authorization.

Data and Privacy - Consumers should be informed of how their data are being transferred through any new payment system, including what data are being transferred, who has access to the data, how that data can be used, and potential risks. As appropriate, consumers should be permitted to specify what data can be transferred and whether third parties can access that data, and protections against misuse of the data associated with payment transactions should be provided.

Fraud and Error Resolution Protections - Consumer protections should be provided with respect to mistaken, fraudulent, unauthorized, or otherwise erroneous transactions. Information should be created and recorded to facilitate post-transaction evaluation, and mechanisms should be available for reversing erroneous and unauthorized transactions quickly once identified.

Transparency - Real-time access to information about the status of transactions should be available, including confirmations of payment and receipt of funds. Timely disclosure of the costs, risks, funds availability, and security of payments is provided.

Cost - Fees charged to consumers should be disclosed in a manner that allows consumers to compare the costs of using different available payment options. For any system, fee structures should not obscure the full cost of making or receiving a payment.

Access - Faster payment systems should be widely accepted by businesses and other consumers to ensure broad accessibility and usability. Consumer access should be available through qualified intermediaries and other non-depositories (such as mobile wallet providers and payment processors) except to the extent necessary to protect functionality, security, or other user values.

Funds Availability - Guaranteed access to funds should be provided.

Security and Payment Credential Value - Faster payment systems should have strong built-in protections to detect and limit errors, unauthorized transactions, and fraud. They should also limit the value of consumer payment credentials through the use of tokens or other tools, which is expected to limit the worth of security breaches to the perpetrators of fraud and minimize the harm to consumers.

Strong Accountability Mechanisms that Effectively Curtail System Misuse - The goals and incentives of system operators, commercial participants, and end users should be aligned against misuse. Commercial participants should be accountable for the risks, harm, and costs they introduce to payment systems and incentivized to prevent and correct fraudulent, unauthorized, or otherwise erroneous transactions for consumers. Systems should also have automated monitoring capabilities, incentives for participants to report misuse, and "transparent" enforcement procedures.

Regulatory Interest in Payment Processors

Payment processors can be subject to CFPB oversight as both "covered persons" and "service providers." The CFPB has taken a number of actions against payment processors to further consumer protection efforts. These include, among others:

- A legal complaint filed in U.S. District Court against a group of debt collectors, their companies, and their service providers to address the CFPB's allegations they violated the law, including the CFPA UDAAP provisions, by attempting to collect debts that were not owed to them and by harassing and lying to consumers in that process. The CFPB alleges the operation depended on the participation of their payment processors, which facilitated debit and credit card payment capability. The complaint states that the payment processors failed to conduct "reasonable due diligence to detect the unlawful conduct of

the debt collectors," approved merchant applications that contained "indicia of fraud," and "ignored warnings from industry and consumers that the payment processors' clients were engaged in a scheme to defraud consumers." As such, the CFPB finds that the payment processors "knew, or should have known" that the debt collectors were engaged in unlawful conduct and so, they "knowingly or recklessly provided substantial assistance" to a covered person or service provider in violation of the CFPA. The relief sought by the CFPB in the complaint includes injunctive relief, civil money penalties, disgorgement or compensation for unjust enrichment, and "such relief as the Court finds necessary to redress injury to consumers" including rescission or reformation of contract, refunds, restitution and damages.

- A legal complaint filed in U.S. District Court against a debt-settlement payment processor to address the CFPB's allegations the payment processor helped other companies to collect illegal upfront fees from consumers in violation of the Telemarketing Sales Rule. The complaint alleged that the payment processor transmitted advance fees for consumers that "it knew, based on its own account records," it had not yet transmitted funds to a creditor to settle the consumers' debts and so also knew that the companies were not entitled to an advance fee. The payment processor entered into a Consent Order with the CFPB and agreed to pay $6 million in relief to consumers and a $1 million civil money penalty.
- The filing of proposed consent orders in federal court to settle charges against two telecommunications companies that allegedly permitted third-parties (i.e., merchants) to place unauthorized charges on the account billing statements of the companies' customers. The Bureau is charging each of the companies, as payments processors for their third parties, with violations of the UDAAP provisions of the CFPA. Collectively the companies agreed to pay approximately $120 million in redress to customers, and one of the companies must also pay approximately $38 million in federal and state fines.

The Federal Deposit Insurance Corporation ("FDIC") issued guidance (Financial Institution Letter (FIL) 41-2014, July 28, 2014) governing its supervisory approach to institutions establishing account relationships with third-party payment processors, which are entities that process payments for "merchants" (e.g., telemarketers, online businesses). The guidance states these relationships can pose risks to institutions that require due diligence and ongoing monitoring. In addition, the guidance states:

- Account relationships with high-risk entities pose increased risks, including potential violations of Section 5 of the FTC Act.
- Certain types of payment processors may pose heightened money laundering and fraud risks if merchant client identities are not verified and business practices are not reviewed.
- Financial institutions should assess risk tolerance in their overall risk assessment program and develop policies and procedures addressing due diligence, underwriting, and ongoing monitoring of high-risk payment processor relationships.
- Financial institutions should be alert to consumer complaints or unusual return rates that suggest the inappropriate use of personal account information and possible deception or unfair treatment of consumers.
- Financial institutions should act promptly when fraudulent or improper activities occur relating to a payment processor, including possibly terminating the relationship.
- Improperly managing these risks may result in the imposition of enforcement actions, such as civil money penalties or restitution orders.

The CFPB issued Bulletin 2012 – 03 (April 13, 2012), which provides guidance related to the Bureau's expectation that supervised banks and nonbanks oversee their business relationships with their service providers in a manner that ensures compliance with the applicable Federal consumer financial laws. In some cases, the legal responsibilities for failure to comply with the laws or to protect consumers may lie with the supervised bank or nonbank in addition to the liability assigned to the service provider. The guidance suggests that oversight of service providers should include:

- Conducting due diligence to ensure the service provider understands and is capable of complying with the relevant Federal consumer financial laws;
- Reviewing the service providers policies, procedures, internal controls, and training materials;
- Including terms in the contract to require compliance with Federal consumer financial laws;
- Establishing controls and ongoing monitoring of the service provider's compliance with Federal consumer financial laws; and
- Promptly addressing any identified problem.

Commentary

A variety of factors are converging to increase regulatory concern with payment systems. On one hand, the industry is experiencing:

- Increasing reliance on electronic payments across demographics;
- Growth in payments through the Internet;
- Increasing adoption of alternate payments routes, such as mobile payments;
- Shifting demographics; and
- Partnerships between banks and nonbanks.

On the other hand, the industry is pressured by:

- Consumer and merchant preferences;
- Cross-channel access;
- Increased fraud risk;
- Regulatory change; and
- Heightened compliance expectations from regulators and financial institutions alike.

These pressures will only increase as new products and faster payment systems are introduced and the expectations / demands of payment stakeholders, especially consumers, increase accordingly. As "covered persons" or "service providers" that fall under the authority of the CFPB, it is critical for payment processors to begin to evaluate their own operations in light of the CFPB's supervisory expectations, which focus on consumer protection and business conduct throughout the lifecyle of business activities, from product development through to ongoing customer touch points and interactions. Rather than thinking of "payment processing" within silos by product set, the CFPB's expectations require a broader view of "payment processing" that entails:

- Being proactive about the underlying spirit of the regulations and focusing on the principles of fair and responsible banking activities;
- Taking an enterprise-wide approach to compliance management and embedding compliance risk management into the business processes; and
- Viewing the current regulatory interest in the payment process as an opportunity to develop an enterprise-wide compliance culture for the management of risks associated with all relevant laws and regulations, ethics standards and non-compliance risks such as operational risk, strategic risk, legal risk, and reputation risk.

CFPB guidance (and that of the prudential regulators) expects supervised banks and nonbanks to oversee relationships with their service providers (or merchant customers in the case of payments processors) to ensure the service providers comply with federal consumer financial laws and operate in a manner that protects consumers and avoids consumer harm. Legal responsibilities for failure to comply with the laws or to protect consumers, in some cases, may lie with the supervised bank or nonbank in addition to the service provider – and this has been borne out by many of the CFPB's enforcement actions.

The CFPB expects each entity to have an effective compliance management system ("CMS") that is adapted to its business strategy and operations. The CFPB also expects bank and nonbank entities to meet the same standards and will evaluate all entities under the same procedures to the extent practicable. CFPB examinations include review and testing of components of an entity's CMS (such as, board of director oversight, the compliance management program, responses to consumer complaints, and audit coverage), and each provider is expected to "address and prevent violations of law and associated harms to consumers through its compliance management process." Accordingly, payment processors should ensure they have a robust CMS in place, including policies, procedures, internal controls, training, and monitoring requirements, to promote compliance with federal consumer financial laws, including UDAAP, as well as to ensure they have conducted appropriate due diligence and ongoing monitoring to "know" the nature and purpose of their merchant customers' businesses.

Regulatory expectations have been heightened to the point that "good" is no longer "good enough" and consumer protection must now be at the forefront of decision-making. Both depository financial institutions and payment processors should expect increased regulatory oversight, expanded regulatory expectations, and an increase in legal actions. In anticipation, particular attention should be given to the areas of:

- Account relationships;
- Unauthorized payments;
- Payments processing and application;
- Fees;
- Data privacy and security;
- Dispute and complaint resolution;
- Fraud monitoring;
- Bank Secrecy Act / Anti-money laundering;
- Information reporting and technology;
- Third-party oversight and vendor management;
- Compliance management system; and
- Regulatory change management.

This is a publication of KPMG's Financial Services Regulatory Risk Practice and the Americas Financial Services Regulatory Center of Excellence (CoE).

For additional information please contact:
Amy Matsuo, Principal: amatsuo@kpmg.com
Kari Greathouse, Principal: cgreathouse@kpmg.com
Ursula Nigrelli, Director: unigrelli@kpmg.com

Author:
Karen Staines, Director, Americas Financial Services Regulatory CoE: kstaines@kpmg.com

Earlier editions are available at:
www.kpmg.com/us/regulatorypracticeletters

The Americas Financial Services Regulatory CoE is based in Washington, DC and comprised of key industry practitioners and regulatory advisers from across KPMG's global network.