VENABLE LLP

client alert

AUTHORS:

D. E. Wilson, Jr.
dewilson@Venable.com
202.344.4819

Ellen Traupman Berge
etberge@Venable.com
202.344.4704

Andrew E. Bigart
aebigart@Venable.com
202.344.4323

Squeezed From All Sides: Payment Processors in the New Regulatory Environment

Being a successful part of the payment processing business in the rapidly changing and growing credit, debit and prepaid landscape has never been easy. The business model shifts almost daily, requiring flexibility and agility in every aspect of the enterprise. The evolving—and multiple—mobile payment platforms alone illustrate the dynamism in the industry.

Parallel to these business pressures are regulatory ones. At the federal level, each of the regulators with oversight of the processing industry—the Office of the Comptroller of the Currency (OCC), the Federal Reserve Board (FRB), the Federal Deposit Insurance Corporation (FDIC), the Consumer Financial Protection Bureau (CFPB), the Federal Trade Commission (FTC), and the National Credit Union Administration (NCUA)—has an important role to play in ensuring a safe and sound financial system and protecting consumers.

These regulators are "complemented" by others at the federal and state levels. Federally, the Financial Crimes Enforcement Network (FinCEN) and the Office of Foreign Assets Control (OFAC), both part of the Treasury, oversee anti-money laundering laws and the United States' economic sanctions against countries such as Iran and Syria. The Department of Justice (DOJ) has interagency working groups focused on each level of payment processing—Interagency Bank Fraud; Mass-Marketing Fraud; Mortgage Fraud; Identity Theft Fraud; and the Consumer Protection Initiatives Committee. Finally, the U.S. Secret Service (USSS), Federal Communications Commission (FCC), and others (including intelligence agencies) play important roles in the data security and mobile payments areas.

Recent events illustrate the scope of regulatory compliance and enforcement pressures being imposed on the payments sector. Beginning in 2013, and receiving national attention, has been DOJ's Operation Chokepoint, focusing on banks as the "gatekeepers" to the financial system. A major concentration of Operation Chokepoint's efforts has been on payment processors, as illustrated in the Four Oaks Bank matter.[1]

More recently, another massive data breach occurred, impacting millions of consumers. According to *The New York Times*, the cyber attack on JP Morgan Chase—still unfolding—touched more than 83 million households and businesses and involved "about nine other financial institutions."[2]

Top Down: Traditional Financial Regulators

The traditional banking agencies—the OCC, FDIC, FRB, and NCUA—are responsible for the safety and soundness of the financial system. From these agencies' perspective, any participant in the payment process affiliated with a financial institution (FI) (and what "participant" is not?) is subject

---

[1] *United States Attorney Announces Settlement with Bank Accused of Consumer Fraud*, April 29, 2014, http://www.justice.gov/usao/nce/press/2014/2014-apr-29.html

[2] http://dealbook.nytimes.com/2014/10/03/hackers-attack-cracked-10-banks-in-major-assault/?_php=true&_type=blogs&_php=true&_type=blogs&_r=1& (Oct. 3, 2014, 9:39 p.m.)

to supervision and enforcement by the appropriate federal bank regulatory agency. "Affiliates" include a very broad range of companies—any company the products and services of which are offered through, associated with, or otherwise facilitated by a "federally insured depository institution." This means any FI that is (a) charted by the OCC (including the Office of Thrift Supervision) or NCUA, (b) a member of the FDIC, or (c) regulated by the FRB. Only a handful of FIs are not subject to federal oversight and examination.

To the extent participants in the payment system (processors, acquirers, providers of prepaid access, *etc.*) are under the impression that the focus on third-party actors in the FI world is new, they need to review the history of this regulatory issue. For example, the OCC made clear in guidance issued in 2001 it will not hesitate to extend its enforcement jurisdiction to third-party service providers that:

1 Perform functions on the bank's behalf;

2. Provide products and services that the bank does not originate; or

3. Utilize a relationship with a national bank to "franchise" the bank's attributes (*i.e.*, use the bank's charter to facilitate the delivery of certain products and services).[3]

The OCC's 2001 guidance takes a broad view of what constitutes a third-party service provider subject to its oversight.[4] These providers are subject to direct examination by the OCC and other member of the Federal Financial Institutions Examinations Council (FFIEC) under the Bank Service Company Act.[5] Finally, the guidance sets out how contractual relationships with third-party service provides should be structured, maintained and monitored.

These requirements were updated and amplified by the OCC in late 2013[6] and are emphasized throughout the FFIEC guidance.[7] The failure of FIs to abide by these rules is, from the regulators' perspective, a major reason for Operation Chokepoint and the increasing enforcement focus on FIs' third-party relations, as well as the related forms of oversight by other agencies, such as the USSS, the FTC, and the FCC.

In short, any entity having a relationship with a federally insured depository institution as a service provider is subject to regulation and examination by traditional bank regulators. In fact, since the formation of the CFPB, the traditional regulators appear to have taken their responsibilities in this area more seriously, forming the first side of the "squeeze."

Bottom Up: The CFPB

The second "squeeze" comes from the bottom up. The CFPB has a singular focus on the consumer, and was formed in the wake of the latest recession to counter the perceived lack of a consumer financial protection system with "sufficiently effective rules or consistent enforcement."[8] So, while bank regulators examine payment processors for "safety and soundness" because they are affiliated with FIs, the CFPB is looking to regulate and examine the same companies from "the consumer's perspective."

For example, at the end of 2012, the CFPB issued a "Request for Information Regarding Credit Card

---

[3] OCC Bulletin 2001-47, November 1, 2001, at http://www.occ.gov/news-issuances/bulletins/2001/bulletin-2001-47.html

[4] *Id.*, footnote 3, "Third parties subject to this guidance may be bank or nonbank, regulated or non-regulated, foreign or domestic, affiliated or independent."

[5] 12 USC 1867(c).

[6] Third-Party Relationships: Description: Risk Management Guidance, OCC Bulletin 2013-29 (October 30, 2013). http://www.occ.gov/news-issuances/bulletins/2013/bulletin-2013-29.html

[7] www.ffiec.gov.

[8] Consumer Financial Protection Bureau, Strategic Plan FY 2013-FY 2017, Goal 1 (www.consumerfinance.gov/strategic-plan)

Market."[9] As required by the Credit Card Accountability and Disclosure Act (CARD Act)[10], this notice solicited information about a number of aspects of the consumer credit card market. The data gathered from this review will form the basis for addition regulations, targets of regulation, and enforcement proceedings.[11]

The coming regulations will also build on three major enforcement actions brought by the CFPB against credit card companies and directed at marketing and debt collection practices the CFPB considers deceptive, unfair or abusive.[12] From the CFPB's intensely consumer-oriented perspective, the new regulations will place compliance obligations on parts of the prepaid industry that ordinarily have no consumer-related responsibilities.

For professionals who have lived through the increased responsibilities placed on FIs to enforce government rules in areas such as anti-money laundering, politically-exposed persons, and economic sanctions, the impact here is likely to be the same. Participants in the processing business will probably see regulatory obligations that are tangential to their businesses, but will be a cost of staying in the processing game. It remains to be seen if these new regulations will take into account business realities or work well with current bank regulatory requirements.

From the Sides: Justice, the FTC, Self-Regulation and Everything Else.

The final "squeeze" comes from multiple sources—DOJ, FTC, other federal and state regulators, and the payment industry's various self-regulatory bodies. For example, payment processors traditionally provide service under the umbrella of banking regulatory guidance issued to their sponsoring banks. Processors, however, also operate in compliance with voluminous operating regulations issued by the various card brands, Payment Card Industry Data Security Standards, and FinCEN and OFAC requirements as to anti-money laundering and economic sanctions.

On top of these regulatory requirements, the FTC expects processors to serve as the first line of defense against marketing practices and consumer products and services the FTC deems problematic. In this role, it could be said that a processor is now expected to pass judgment on its merchant clients, refuse service to or terminate "bad" merchants, and report non-compliant merchants—not only to terminated merchant files [such as the Member Alert to Control high-risk Merchants (MATCH) list], but also to law enforcement. The FTC has sought to hold processors responsible for the total volume of sales processed by such merchants, thereby making processors guarantors for consumer transactions. Moreover, the injunctive provisions present in FTC settlements with processors have included outright bans on servicing various types of high-risk merchants and near-debilitating conditions on processing for other merchants.[13] (For its part, the CFPB has also brought enforcement actions against payment processors, including in two separate matters involving the debt settlement industry.[14])

Beyond the FTC, other federal and state agencies, as well as self-regulatory bodies, further complicate the regulatory landscape. At the federal level, the DOJ task forces coordinate law enforcement and prosecutions across federal, state and local jurisdictions. FinCEN, responsible for the anti-money laundering laws, will likely issue regulations in the coming months requiring FIs to know and verify the identities of real people who own, control and profit from entities' FI services.[15]

---

[9] https://www.federalregister.gov/articles/2012/12/20/2012-30609/request-for-information-regarding-credit-card-market. This comment period closed on February 19, 2013

[10] 15 U.S.C. § 1616(a).

[11] *Strategic Plan*, n.8, Goal 3.

[12] Steven Forry, *2012: The CFPB Set its Sights on Credit Card Companies*, Business Law Today (March 22, 2013)

[13] *See, e.g.*, http://www.ftc.gov/system/files/documents/cases/140611iwbstiporder.pdf (FTC settlement with IRN Payment Systems resulting in $3.48 million monetary judgment and ban on processing for any merchants selling debt relief products or services).

[14] *See, e.g.*, http://www.consumerfinance.gov/newsroom/cfpb-takes-action-against-meracord-for-processing-illegal-debt-settlement-fees/.

[15] http://www.treasury.gov/press-center/press-releases/Pages/jl2595.aspx

When final, this rule may require payment processors to disclose their ownership structures to their FIs and to obtain similar information from the merchants they service—unless FinCEN adopts a provision allowing FIs to share account Customer Identification Process information. FinCEN's sister Treasury agency, OFAC, continues to enforce the economic sanctions laws against FIs, their affiliates and other U.S. individuals and companies.[16]

State attorneys general remain active in enforcing consumer protection laws, and the states' regulations and enforcement actions will evolve with the federal regulation. Finally, self-regulatory bodies will continue to find ways both to establish cross-industry standards that add protection in the electronic payments world,[17] and to anticipate federal and state bank-affiliate and consumer protection regulations.

Conclusion

The impacts of this renewed focus on "intermediary companies" in the consumer finance world are:

1. Regulatory uncertainty that will lead to increased operational costs;

2. Increased attention to a broad set of potential regulatory and examination risks that require higher levels of internal compliance and audit by industry participants; and

3. Adjustments in external relations to demonstrate compliance with the emerging sets of regulations and compliance pressures.

[16] *E.g.*, http://www.treasury.gov/resource-center/sanctions/CivPen/Documents/20140724_bofa.pdf [$16,562.700 settlement for "apparent" Bank of America violations of the Foreign Narcotics Kingpin Sanctions Regulations (July 24, 2014)]; http://www.treasury.gov/resource-center/sanctions/CivPen/Documents/20140909_zulutrade.pdf ($200,000 to settle potential civil liability for Zulutrade, Inc., apparent violations of Iran, Sudan and Syria economic sanctions.).

[17] An example here is, of course, PCI SSC (www.pcisecuritystandards.org) that sets the PCI Data Security Standard.