Client Alert | Financial Institutions / Regulatory & Compliance

Payment Processor Risk: Do You Know It When You See It? Red Flags for the Unwary

September 2016

Authors: **Kevin Petrasic**, **Benjamin Saul**, **Helen Lee**, **Joshua Garcia**

Recent litigation and enforcement activities of the Consumer Financial Protection Bureau ("CFPB" or the "Bureau") spotlight the heightened regulatory focus on payment intermediaries, *i.e.* processors, and their role as "gatekeepers."

In the CFPB's words, expressed in the Bureau's recently filed complaint against payment processor Intercept Corporation and its principals ("Intercept"), payment processors provide "access to the banking system" and the means for businesses—including potentially unscrupulous ones—to extract money from consumers' bank accounts.[1] In opposition to Intercept's efforts to dismiss the CFPB's action, the Bureau reemphasized the unique position of payment processors and their attendant responsibilities, noting that, "[a]s gatekeepers to a system in which so much money changes hands, third-party payment processors as well as the banks they work with have responsibilities to monitor their transactions for suspicious activity and not enable fraud on the ACH network."[2]

Beyond the *Intercept* matter, the CFPB's lawsuits in recent years against telecommunications giants Sprint and Verizon showcase the need for payment intermediaries, including entities whose payment processing activities are incidental to their core business, to remain vigilant in the face of increased regulatory scrutiny. Collectively, these matters, along with the CFPB's recent settlements involving payment processors, highlight the importance of maintaining adequate compliance and monitoring systems. Discussed below are further details regarding the CFPB's litigation and enforcement activities against payment processors, compliance issues showcased by such matters, and pro-active risk mitigation strategies that payment processors should consider in light of recent CFPB scrutiny.

Financial Institutions Advisory

Bank Advisory
Broker-Dealer
Consumer Financial Services
Cybercurrency
Cybersecurity
Data Privacy & Protection
EU and WTO
FinTech
Investment Advisory & Management
Payments
Sanctions, Bank Secrecy and Export Controls
Securities
Trust and Fiduciary

CFPB Jurisdiction Over Payment Processors

In 2011, Congress, under Title X of the Dodd-Frank Wall Street Reform and Consumer Protection Act (the "CFPA"), created the CFPB and charged it with responsibility to enforce the CFPA and other federal consumer financial laws.[3] Under the CFPA, it is unlawful for "any covered person or service provider" to "offer or provide to a consumer any financial product or service not in conformity with Federal consumer financial law, or otherwise commit any act or omission in violation of a Federal consumer financial law;...or to engage in any unfair, deceptive, or abusive act or practice."[4] Moreover, any person who "knowingly or recklessly provide[s] substantial assistance to a covered person or service provider in violation of the [prohibition on unfair, deceptive, or abusive acts or practices]...shall be deemed to be in violation of that section to the same extent as the person to whom such assistance is provided."[5]

A "covered person" includes "any person that engages in offering or providing a consumer financial product or service."[6] A "consumer financial product or service" is in turn defined to include "any financial product or service that is described in one or more categories under [12 U.S.C. § 5481(15)] and is offered or provided for use by consumers primarily for personal, family, or household purposes."[7] The categories of financial products or services described under section 5481(15) include:

> providing payments or other financial data processing products or services to a consumer by any technological means, including processing or storing financial or banking data for any payment instrument, or through any payments systems or network used for processing payments data, including payments made through an online banking system...[8]

Thus, under the CFPA, companies—whether or not they self-identify as payment processors—that engage in the broad category of payment processor activities described above are arguably subject to the CFPB's jurisdiction over covered persons when they engage in that activity for use by consumers primarily for personal, family or household purposes.

Independent from any covered person analysis, the CFPB may also assert jurisdiction over companies that are "service providers" to covered persons, including lenders, debt collectors and other providers of consumer financial products or services,[9] and "related persons," which includes "any director, officer, or employee charged with managerial responsibility for, or controlling shareholder of, or agent for, such covered person."[10]

As noted above, the CFPB also has a jurisdictional means to bring an enforcement action against *any* entities that "knowingly or recklessly provide substantial assistance" to covered persons violating the prohibition against unfair, deceptive, or abusive acts or practices ("UDAAP"), which sweeps in entities that provide such assistance when they know or should have known of the covered person's allegedly harmful activity. As discussed below, the CFPB has asserted that payment processors who know (or consciously avoid knowing) that their customers are charging illegal fees, yet process those fees, provide substantial assistance to covered persons in violation of applicable law.[11] For example, in both the *Intercept* case, and in a 2015 case against payment processor Universal Debt & Payment Solutions, the CFPB leveraged the "substantial assistance" argument to bring actions against executives managing the defendant companies.[12]

The CFPB's novel use of "substantial assistance" highlights the need for clear delineation regarding the Bureau's jurisdictional authority, especially since the provision applies to *any* person and not just covered persons. The CFPA neither defines "substantial assistance" nor does it explain what the CFPB must prove to meet the "knowingly or recklessly" standard. Although it clearly states that UDAAP violations are a predicate offense, the CFPB has settled claims where it alleged entities provided "substantial assistance" to a covered person violating non-UDAAP rules such as the Telemarketing Sales Rule ("TSR") and the Real Estate Settlement Procedures Act ("RESPA").[13] While the TSR has a separate "substantial assistance" grant of authority upon which the CFPB can rely,[14] RESPA does not.

Recent CFPB Actions Against Companies for Payment Processor Activities

The CFPB's recent actions involving payment processors illustrate the Bureau's efforts to pursue and punish payment processors that fail to remain sufficiently alert in their activities as gatekeepers and fail to monitor the activities of their consumer-facing customers.

A. *CFPB v. Intercept Corporation d/b/a InterceptEFT*

On June 6, 2016, the CFPB filed a lawsuit in federal district court against payment processor Intercept Corporation and two of its executives for allegedly enabling unauthorized and other illegal withdrawals from consumer accounts by their merchant clients. The CFPB alleged that Intercept and its principals "turned a blind eye to blatant warning signs of potential fraud or lawbreaking by its clients" and detailed the various occasions where the CFPB found the defendants to have "ignored blatant warning signs of potential fraud" and "ignored complaints from banks and consumers."[15]

The CFPB asserted that it had jurisdiction over Intercept and its principals for their alleged illegal conduct on the basis that they are "covered persons," "related persons" and/or "service providers" within the meaning of the CFPA.[16] The agency also asserted that individual executives of the company knowingly or recklessly provided "substantial assistance" to Intercept as it violated the prohibition against UDAAPs.[17] However, in support of a motion to dismiss the CFPB's complaint, Intercept argued, among other things, that the CFPB lacked jurisdiction over the Intercept defendants because Intercept is neither a "covered person" nor a "service provider," Intercept's principals are neither "covered persons" nor "related persons," and there could be no "substantial assistance" liability because Intercept did not commit a UDAAP violation.[18] Specifically, Intercept argued that, in order for the CFPB to assert the payment processor authority over Intercept, Intercept "must offer its payment processing services directly to consumers to be considered a "covered person," and those services must be used "primarily for personal, family, or household purposes."[19] According to Intercept, since it "does not contract with individual consumers [rather, Intercept's customers were businesses that included lenders, finance companies and debt collectors], and its customers do not use its services for "personal, family, or household purposes," the CFPB's lawsuit against Intercept was improper in that it exceeded the limits of the CFPB's jurisdiction under the CFPA, which "plainly excludes business-to-business companies such as Intercept from its reach."[20]

In response to Intercept's arguments and those offered by the amicus Third Party Payment Processors Association, the CFPB noted that, notwithstanding that Intercept's direct clients are businesses rather than consumers (who, in turn, are clients of those businesses), "the relevant question" is not whether Intercept "contract[s] directly with the consumers whose payments it processed," but rather:

> ...the statutory language asks whether Intercept "provid[ed]" its services "to a consumer"—as required for payment processing to be a "financial product or service" under section 5481(15)—and "for use by consumers" for a personal, family, or household purpose—as required for processing to be a "consumer financial product or service" under section 5481(5). While these provisions obviously contemplate a consumer to whom the services are directed, nothing in the statutory text even implies that a covered person must contract directly with the consumer. When payment processors transmit legitimate credit and debit requests that were authorized by consumers, those processors provide the service of convenient and fast electronic payment processing both "to" and "for use by" consumers regardless of whether they do so directly or via third-party arrangements.[21]

The tenability of the CFPB's position in *Intercept* will be closely watched in terms of how the court decides on Intercept's motion to dismiss. If the court agrees with the CFPB on the covered person jurisdictional issue, such ruling would significantly expand the universe of companies traditionally thought of as providers of consumer financial products or services to include companies offering products and services to businesses with downstream consumers. The CFPB's litigation stance clearly shows its interest in pursuing aggressive action against middlemen such as payment processors, notwithstanding the lack of a direct relationship with consumers.

B. *CFPB v. Sprint Corporation and CFPB v. Cellco Partnership d/b/a Verizon Wireless*

The broad language of the CFPA also enabled the CFPB to treat two telecommunications companies as payment processors. In similar lawsuits that the CFPB filed against Sprint and Verizon (both settled in mid-2015), the CFPB alleged that, although the companies outsourced compliance and payment processing functions to billing aggregators, they each maintained "control over the collection, processing, and distribution of payments"[22] and were "covered persons" for purposes of the CFPA, having each "process[ed] payments for consumers in connection with third-party goods."[23]

The CFPB's complaint alleged that the companies adopted a flawed billing system that permitted third parties to "cram," or place unauthorized charges on, a telecommunication subscriber's mobile phone bill. Among the deficient practices alleged by the CFPB were the companies' practice of automatically enrolling customers into billing systems that exposed them to third-party cramming activities. According to the CFPB, third parties submitted charges to mobile phone bills, billing aggregators placed such charges on customer bills, and the phone companies charged the payments to consumers, receiving approximately 30 to 40 percent of the gross revenue from these charges.

Notably, the phone companies did not initiate the unauthorized charges, which came from unaffiliated businesses claiming to have received the authorization of the phone companies' customers to initiate the charges. However, the phone companies provided the platform for the third-party businesses to initiate the charges and outsourced certain payment processing functionality such as compliance, billing aggregation and fraud prevention. Notwithstanding the outsourced functions, the CFPB argued that the phone companies each exercised a sufficient degree of control with respect to their respective payment processes to be considered "providing payments or other financial data processing products or services" and, perhaps more importantly, profited from the unauthorized payments initiated by others. The phone companies were ordered to pay a combined total of $120 million in consumer redress and $38 million in federal and state fines.[24]

These CFPB actions were noteworthy in that the agency pursued two major telecommunications providers, *i.e.*, companies that are not traditionally considered to be financial service providers, as payment processors offering a consumer financial product or service. The lesson from these actions is that the Bureau's view of payment processing activity is expansive. Companies engaging in similar outsourcing activities should understand that their billing practices for consumer products or services may be scrutinized both for their own actions and for those of their business partners, for which they may be held accountable. In this regard, such companies may wish to review, if they have not done so already, their degree of control over any payment processing functions such as collection, processing and distribution of payments, especially where customers are automatically enrolled in billing systems that permit third-party charges.

Red Flags for Payment Processors

As evidenced by several actions the CFPB has pursued recently, the agency has broad jurisdiction over payment processors' activities that directly and indirectly impact consumers. The agency's reach not only encompasses so-called "traditional" providers of consumer financial products and services—according to the CFPB, its reach also extends to companies providing financial products and services to *businesses* that have a tangential or downstream impact on consumers.

While traditional providers of consumer financial products and services are familiar with consumer protection rules and practices intended to mitigate consumer harm,[25] payment processor companies providing services to businesses and/or operating outside the financial services industry are likely less aware of the heightened supervisory scrutiny and risk attendant to such activities where consumers may be impacted. For instance, in a March 2016 CFPB enforcement action taken against payment processor Dwolla for alleged deceptive data security practices, the CFPB noted that, among other alleged deficient practices, the company did not require applications developed through its affiliated software development operation to comply with the company's own stated security practices and, as a result, exposed consumers to third-party applications without testing for security.[26]

Given this background, it is important for all companies engaging in payment processor activities that potentially impact consumers to watch for red flags[27] that have been highlighted in recent CFPB enforcement actions to ensure that they meet the CFPB's expectations in fulfilling their gatekeeper roles. These red flags include:

- **High Refund Rates.** Where merchants have refund rates that are substantially higher than the relevant industry average for return rates.[28]
- **Date and Amount Discrepancies.** Where a payment processor discovers discrepancies between the dates and amounts debited from consumers' accounts compared to what the consumer had authorized.[29]
- **Customer and Consumer Group Complaints.** Where consumers submit a large number of complaints, especially if they are concentrated in one jurisdiction.[30] For instance, the CFPB alleged in its complaint against Intercept that the company ignored at least 87 complaints from Georgia consumers and 346 complaints from Arkansas consumers.[31] In addition, it would be a red flag where advocacy groups submit complaints on behalf of a large group of consumers, as was the case in the *Sprint* and *Verizon* actions, where a consumer group submitted complaints to both companies about third-party cramming taking place on their respective billing systems.[32]
- **Law Enforcement Actions.** Where a payment processor becomes aware of law enforcement action against its business customers, such as a cease and desist letter[33] or settlements for practices specifically tied to consumer harm (such as cramming).[34]

Payment processors have also been fined for processing illegal fees.[35] In the *Sprint* and *Verizon* actions, the CFPB's rationale was that, although the companies did not initiate the challenged fees in violation of the TSR, they offered a platform on which third parties were able to successfully have those fees processed, and thus were liable for providing "substantial assistance" to the entities charging the illegal fees.[36] In the complaints against Intercept, Sprint and Verizon, the CFPB also argued that when payment processors process illegal or unauthorized fees or unauthorized debits to consumer accounts, they engage in "unfair" acts under the Dodd-Frank Act, in which the CFPB was provided enforcement authority to prevent such UDAAPs.[37]

Adopt a Proactive Stance

The primary takeaway from recent CFPB actions is that the compliance landscape is changing for all payment processors—regardless of whether they serve consumers directly or they serve businesses that serve consumers—when activities or operations have the potential to lead to consumer harm. To respond to this changing landscape, there are a number of actions that companies should consider to adopt a proactive stance toward risk management:

- **Closely Monitor Return Rates.** Payment processors of all types, but particularly those serving riskier industries involving consumer financial services—including consumer lending, debt relief or debt settlement, and debt collection—should periodically monitor return rates of the businesses for which they process payments and develop an action plan for when such rates exceed pre-specified percentages. In this regard, NACHA guidelines emphasize the responsibility of all participants in the ACH system to monitor merchant return rates to detect and prevent fraud; thus, a formal monitoring program may be appropriate.
- **Consider Automated Compliance.** In recent years, regulatory technology (or "regtech") has advanced to offer low-cost automated compliance monitoring solutions. Such technology could easily capture, for example, a change in date or amount authorized from an initial authorization to subsequent authorizations. It could also automatically trigger user-defined limits on merchant access to the payment system or send high-priority alerts once return rates exceed a specified percentage of overall merchant volume.
- **Monitor and Respond to Consumer Complaints.** Payment processors should also have a formal program through which they collect data on consumer complaints (*e.g.*, complaint information about the merchant, merchant's industry and merchant's customer base would all help track trends), as well as a structured consumer complaint response system that assures attention to addressing specific issues evidencing compliance and other program deficiencies.

- **Review Internal Compliance Program.** In order to effectively implement changes and fluidly respond to consumer complaints, payment processors should establish and maintain a robust internal compliance management system. Payment processors should work with third-party vendors to develop and formalize such systems.

- **Review Contractual Provisions**. Ensure that form agreements with prospective customers include standardized provisions—such as a requirement that customers follow applicable law—in order to minimize legal risks. Depending on the risk level of the customer and the compliance system of the payment processor, payment processors may want to strengthen standard provisions regarding audit rights or providing access to consumer complaints.

- **Consider Dialogue with the CFPB or Primary Federal Bank Regulator.** The CFPB has an office, Project Catalyst, specifically dedicated to working with companies developing innovative solutions that affect consumers. The federal banking agencies have similar, albeit less formal, outreach programs. At some point prior to the launch of a new product, it may be helpful to consider approaching the CFPB or other federal banking regulator, as appropriate, to obtain certainty (to the extent possible) as to the potential liability that might arise from a new payment product's features. This option is admittedly not suitable for every situation, but is increasingly an option as regulators become more sophisticated and seek increased communication with the payments industry.

Conclusion

The CFPB has broad authority under the CFPA to take enforcement action against payment processors and has shown a clear willingness to do so. Companies engaging in payment processor activities that impact consumers—whether directly or indirectly—must be aware of the increasing regulatory risks attendant with such activities. Although the precise limits of the CFPB's jurisdiction over payment processors that serve businesses (rather than directly serving consumers) are currently being tested and therefore remain unclear, payment processors engaged in activities that have the potential to result in consumer harm should examine their activities and operations in light of recent CFPB actions to ensure the adequacy of their compliance and risk management systems.

WHITE & CASE

AMERICAS

New York

Ian Cuillerier
Partner
T +1 212 819 8713
E icuillerier@whitecase.com

John Donovan
Partner
T +1 212 819 8530
E jdonovan@whitecase.com

David Johansen
Partner
T +1 212 819 8509
E djohansen@whitecase.com

Ernie Patrikis
Partner
T +1 212 819 8200
E ernest.patrikis@whitecase.com

Duane Wall
Partner Of Counsel
T +1 212 819 8453
E dwall@whitecase.com

Francis Zou
Partner
T +1 212 819 8733
E fzou@whitecase.com

Glen Cuccinello
Counsel
T +1 212 819 8239
E gcuccinello@whitecase.com

Washington, DC

Kevin Petrasic
Partner
T +1 202 626 3671
E kevin.petrasic@whitecase.com

Benjamin Saul
Partner
T +1 202 626 3665
E benjamin.saul@whitecase.com

Jolina Cuaresma
Counsel
T +1 202 626 3589
E jolina.cuaresma@whitecase.com

Helen Lee
Counsel
T +1 202 626 6531
E helen.lee@whitecase.com

EMEA

Frankfurt

Benedikt Gillessen
Partner
T +49 69 29994 0
E bgillessen@whitecase.com

Dennis Heuer
Partner
T +49 69 29994 0
E dheuer@whitecase.com

Matthias Kasch
Partner
T +49 69 29994 0
E mkasch@whitecase.com

Andreas Wieland
Partner
T +49 69 29994 1164
E andreas.wieland@whitecase.com

Hamburg

Kai-Michael Hingst
Partner
T +49 40 35005 364
E kmhingst@whitecase.com

London

Francis Fitzherbert-Brockholes
Partner
T +44 20 7532 1400
E ffitzherbert-brockholes@whitecase.com

Stuart Willey
Partner
T +44 20 7532 1508
E swilley@whitecase.com

Carmen Reynolds
Counsel
T +44 20 7532 1421
E creynolds@whitecase.com

ASIA

Hong Kong

Baldwin Cheng
Partner
T +852 2822 0405
E bcheng@whitecase.com

Sharon Hartline
Partner
T +852 2822 8733
E shartline@whitecase.com

Singapore

David Barwise
Partner
T +65 6347 1345
E dbarwise@whitecase.com

[1] *See CFPB v. Intercept Corporation d/b/a InterceptEFT*, 3:16-cv-00144 (D.N.D. June 6, 2016), Complaint ¶ 2 ("Intercept Complaint").

[2] *CFPB v. Intercept Corporation d/b/a InterceptEFT*, 3:16-cv-00144 (D.N.D. June 6, 2016), Memorandum in Opposition of Defendants' Motion to Dismiss (filed Aug. 29, 2016), pgs. 27-32 ("CFPB Reply Brief").

[3] Title X of the Dodd-Frank Act, entitled the Consumer Financial Protection Act, Pub. L. 111-203, codified at 12 U.S.C. 5301 *et seq*.).

[4] 12 U.S.C. §§ 5536(a)(1)(A) and (B).

[5] 12 U.S.C. § 5536(a)(3).

[6] 12 U.S.C. § 5481(6).

[7] 12 U.S.C. § 5481(5).

[8] 12 U.S.C. § 5481(15)(A)(vii).

[9] The term "service provider" is defined in relevant part as "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…processes transactions relating to the consumer financial product or service." 12 U.S.C. § 5481(26). A company can be both a "covered person" and a "service provider." 12 U.S.C. § 5481(26)(C).

[10] 12 U.S.C. § 5481(25)(i).

[11] *CFPB v. Global Client Solutions LLC*, 2:14-cv-06643 (C.D. Cal. Aug. 25, 2014) Complaint ¶ 24 ("GCS Complaint"); *CFPB v. Meracord LLC*, 3:13-cv-05871 (W.D. Wash. Oct. 3, 2013), Complaint ¶ 20 ("Meracord Complaint").

[12] Intercept Complaint ¶ 132; *CFPB v. Universal Debt & Payment Solutions, LLC*, 1:15-cv-0859 (N.D. Ga. Mar. 26, 2015) Complaint ¶ 325.

[13] See GCS Complaint ¶ 24 (alleged violation of TSR); Meracord Complaint ¶ 20 (alleged violation of TSR); *CFPB v. Genuine Title LLC*, No. 15-cv-1235 (D. Md. April 29, 2015), Complaint ¶¶ 60-63 (alleged violation of RESPA).

[14] 16 C.F.R. 310.3(b).

[15] CFPB Press Release, Consumer Financial Protection Bureau Sues Payment Processor For Enabling Unauthorized Withdrawals And Other Illegal Acts By Clients (June 6, 2016), *available at* http://www.consumerfinance.gov/about-us/newsroom/consumer-financial-protection-bureau-sues-payment-processor-enabling-unauthorized-withdrawals-and-other-illegal-acts-clients/.

[16] Intercept Complaint ¶ 125.

[17] Intercept Complaint ¶ 134.

[18] *CFPB v. Intercept Corporation d/b/a InterceptEFT*, 3:16-cv-00144 (D.N.D. June 6, 2016), Memorandum of Law in Support of Defendants' Motion to Dismiss the Complaint (filed Aug. 8, 2016), pgs. 27-32 ("Intercept Motion to Dismiss").

[19] Intercept Motion to Dismiss, pg. 28.

[20] *Id*.

[21] CFPB Reply Brief, pgs. 9-10.

[22] *CFPB v. Cellco Partnership d/b/a Verizon Wireless*, 3:15-cv-03268 (D.N.J. May 12, 2015), Complaint ¶ 31 ("Verizon Complaint"); *CFPB v. Sprint Corporation*, 1:14-cv-09931 (S.D.N.Y. December 17, 2014), Complaint ¶ 32 ("Sprint Complaint").

[23] Verizon Complaint ¶ 10; Sprint Complaint ¶ 9.

[24] *See generally* CFPB News Release, Sprint and Verizon will refund $120 million to consumers harmed by illegal billing practices (May 12, 2015), *available at* http://www.consumerfinance.gov/about-us/blog/sprint-and-verizon-will-refund-120-million-to-consumers-harmed-by-illegal-billing-practices/.

[25] For example, the financial services industry has long been aware that some industries are riskier to service than others. Regulators, law enforcement agencies and self-regulatory organizations including the Financial Crimes Enforcement Network, the Federal Financial Institution Examinations Council, NACHA (National Automated Clearing House Association), and bank partners and major credit card payment networks have issued guidelines warning about the attendant risks involved in developing relationships with inherently risky industries. *See, e.g.*, FIN-2012-A010 ("The risk profile of [merchant clients of payment processors] can vary significantly depending on the composition of their customer base. For example, Payment Processors providing consumer transactions on behalf of telemarketing and Internet merchants may present a higher risk profile to a financial institution than would other businesses."); FFIEC Bank Secrecy Act/Anti-Money Laundering Examination Manual, Third-Party Payment Processors—Overview ("While payment processors generally affect legitimate payment transactions for reputable merchants, the risk profile of such entities can vary significantly depending on the make-up of their customer base."); and NACHA Risk Management Advisory Group: Sound Business Practices for Evaluating Consumer Risk, 6, *available at* https://www.nacha.org/system/files/resources/RMAG%20Evaluating%20Customer%20Risk%20SBPs%20FINAL.pdf ("Identify concerns for business types defined as more likely to pose an elevated level of risk and determine what actions should be taken to address those concerns.").

[26] 2016-CFPB-0007, March 2, 2016, Dwolla Consent Order ¶¶ 41-46 (noting that "Respondent [Dwolla] failed to test the security of the apps on Dwollalabs.com prior to releasing the apps to the public to ensure that consumers' information was protected").

[27] The CFPB has signaled what it considers red flags for payment processors serving the industries of consumer lending (including payday, auto title, and sales finance), debt collection, debt-relief programs and debt settlement. Notwithstanding that these red flags were developed and derived from enforcement actions against participants in industries known to be more susceptible to a higher risk of consumer harm, such red flags should be observed by all payment processors, regardless of the industry for which they process payments.

[28] For example, the CFPB alleged that refund rates for certain merchants ranged from 20 to 50 percent in the Sprint Complaint and alleged annual return rates ranging from 20 to 40 percent (compared to an industry average of 1.5 percent) in the Intercept Complaint. Sprint Complaint ¶ 30 and Intercept Complaint ¶¶ 76-77 (the CFPB used the industry average from 2012 in its complaint).

[29] Intercept Complaint ¶ 41.

[30] Intercept Complaint ¶ 53.

[31] Intercept Complaint ¶¶ 53, 54.

[32] Verizon Complaint ¶ 5; Sprint Complaint ¶ 4.

[33] Intercept Complaint ¶ 53.

[34] Sprint Complaint ¶ 28.

[35] GCS Complaint ¶ 16; Meracord Complaint ¶ 16.

[36] GCS Complaint ¶ 24; Meracord Complaint ¶ 20.

[37] Intercept Complaint ¶ 129; Verizon Complaint ¶ 35; Sprint Complaint ¶ 37.