

Alert

CFPB Sues Payment Processors for Failing to Detect Fraud Committed by Others

April 10, 2015

This week the Consumer Financial Protection Bureau (“CFPB”) announced the first-ever civil enforcement action alleging that payment processors substantially assisted in a fraud because they processed debit and credit payments by consumers who were tricked out of their money by phony debt collectors who targeted the victims through robo-calls.¹ Although the CFPB does not allege that the payment processors were complicit in the phony debt collectors’ scheme, it nonetheless seeks to hold the payment processors responsible for assisting in the fraud because they “knew, or should have known, that the Debt Collectors were engaged in unlawful conduct.”² In other words, the payment processors are alleged to have enabled the fraud because they failed to respond to red flags and identify those transactions as fraudulent.

The Complaint, filed under seal on March 26, 2015 and unveiled earlier this week, describes a scheme where debt collectors, using aliases and placing automated phone calls to consumers, deceived them into believing that they had to pay debts that they in fact did not owe. According to the Complaint, the calls were threatening and harassing, and were achieved through a telemarketing company.

In announcing the enforcement action, CFPB Director Richard Cordray noted that in the regulators’ view, the payment processors shared culpability with those actors who are alleged to have designed and carried out the underlying fraud: “The ringleaders of the scheme, the telemarketing company that broadcast millions of robo-calls, and the companies that processed the payments should all be held accountable for taking advantage of vulnerable consumers.”³

The CFPB’s Complaint charges four entities for their role in processing the fraudulent transactions: (1) Electronic Merchant Services (“EMS”); (2) Global Payments Inc. (“Global Payments”); (3) Pathfinder Payment Solutions (“Pathfinder”); and (4) Frontline Processing Corp. (“Frontline”). While EMS and Global Payments are themselves payment processors, Pathfinder and Frontline are independent sales organizations that contract with Global Payments to provide marketing services, as well as screening and monitoring processing activity to detect fraud and manage risk.

¹ *Consumer Financial Protection Bureau v. Universal Debt & Payment Solutions LLC, et al.*, 1:15-cv-0859 (N.D.G.A. March 25, 2015).

² Compl. ¶ 3.

³ CFPB, Press Release, “[CFPB Sues Participants in Robo-Call Phantom Debt Collection Operation](#)” (April 8, 2015).

According to the Complaint, each of these entities is a “covered person” and a “service provider” under the Consumer Financial Protection Act (“CFPA”), 12 U.S.C. §§ 5481(15)(A)(vii), (26). The Complaint alleges that the payment processors violated the CFPA in two ways. First, they “knowingly or recklessly provided substantial assistance” to the unlawful conduct of the debt collectors, under 12 U.S.C. § 5536(a)(3).⁴ Second, their practices constituted “unfair acts or practices,” under 12 U.S.C. § 5531(a) and (c)(1), and 5536(a)(1)(B), in that they provided material services to the debt collectors and failed to conduct reasonable due diligence that would have detected the debt collectors’ unlawful conduct, and this caused, or was likely to cause, “substantial injury to consumers that was not reasonably avoidable by consumers and was not outweighed by countervailing benefits to consumers or completion.”⁵

The Complaint alleges that the payment processors facilitated the fraud in part because by enabling the debt collectors to accept credit and debit card payments, the payment processors gave the debt collectors an “air of legitimacy,” which helped convince consumers that the debt collectors were credible merchants.⁶ The Complaint also maintains that the payment processors are liable in part because they violated their own policies and procedures designed to minimize their own credit exposure that results from chargebacks associated with disputed or fraudulent charges.⁷ In other words, the CFPB alleges that if the payment processors were following their own policies and procedures, they should have picked up on the red flags that the debt collectors’ activities presented.

According to the payment processors’ policies, collection agencies are high-risk or prohibited merchants that warrant enhanced scrutiny, but the Complaint alleges that none was applied. The Complaint further alleges that Pathfinder and Frontline (on behalf of Global Payments) and EMS were each deficient in their underwriting and risk monitoring, and the Complaint sets forth a series of facts and circumstances that, if properly monitored and investigated by Pathfinder and Frontline, would have alerted them to the fraud.⁸ The Complaint also alleges that Global Payments, Frontline and Pathfinder failed to monitor the recurring chargeback activity that should have raised red flags and alerted them to the fraud.⁹

In concept, the Complaint is similar to the U.S. Department of Justice’s “Operation Choke Point” initiative, which sought to hold banks responsible for failing to stop third-party payment processors from making ACH withdrawals. Both enforcement strategies target parties who may not be participating in illegal activity but are deemed responsible because they should have known the conduct was illegal and acted to prevent it rather than facilitate it. But the CFPB’s Complaint is also consistent with a larger trend in the current enforcement environment, especially in the financial services industry, where the failure to monitor suspicious activity and respond to red flags can carry more serious consequences than the underlying conduct that went unchecked.¹⁰

⁴ Compl. ¶ 327.

⁵ Compl. ¶¶ 331-35.

⁶ Compl. ¶¶ 5, 144-51.

⁷ Compl. ¶¶ 152-64.

⁸ Compl. ¶¶ 162-218, 247-85.

⁹ Compl. ¶¶ 219-46.

¹⁰ In a similar vein, in 2013 the Federal Trade Commission (“FTC”) issued a Notice of Proposed Rulemaking that, if finalized, would amend the FTC’s Telemarketing Sales Rule, 16 C.F.R. Part 310, to prohibit telemarketers from accepting or requesting certain types of “novel” payment methods. 78 Fed. Reg. 41200 (July 9, 2013). However, the existing Telemarketing Sales Rule prohibits third parties from “provid[ing] substantial assistance or support to any seller or telemarketer when that person knows or consciously avoids knowing that the seller or telemarketer is

Authored by [Seetha Ramachandran](#) and [Joseph P. Vitale](#).

If you have any questions concerning this *Alert*, please contact your attorney at Schulte Roth & Zabel or one of the attorneys in the firm's [Bank Regulatory Group](#).

This information has been prepared by Schulte Roth & Zabel LLP ("SRZ") for general informational purposes only. It does not constitute legal advice, and is presented without any representation or warranty as to its accuracy, completeness or timeliness. Transmission or receipt of this information does not create an attorney-client relationship with SRZ. Electronic mail or other communications with SRZ cannot be guaranteed to be confidential and will not (without SRZ agreement) create an attorney-client relationship with SRZ. Parties seeking advice should consult with legal counsel familiar with their particular circumstances. The contents of these materials may constitute attorney advertising under the regulations of various jurisdictions.

Schulte Roth&Zabel

New York | Washington DC | London

www.srz.com

engaged in any act or practice that violates ... the [Telemarketing Sales] Rule." 16 C.F.R. § 310.3(b). If the proposed amendment ever takes effect, it is likely to be the FTC's view that providing one of the prohibited novel payment methods to a telemarketer constitutes providing "substantial assistance" to that telemarketer because the payment method is directly related to the violation. Therefore, the proposed amendment would impose a new duty on payment processors to determine whether a recipient of a payment is a telemarketer, a seller engaged in telemarketing or an agent for either entity (a difficult if not impossible exercise) and, if so, to deny the transfer absent compelling evidence that the transfer is not payment for goods or services offered or sold through telemarketing.