LOEB & LOEB LLP

Consumer Protection Defense Law

ALERT

DECEMBER 2013

LOEB & LOEB adds Knowledge.

FTC Cracks Down on Payment Processors

The Federal Trade Commission is intensifying its regulatory and enforcement focus on payment processors and payment methods that the agency believes enable illegal telemarketing and other consumer fraud schemes by facilitating unauthorized charges to consumer credit cards and automatic debits from bank accounts.

Earlier this year, the agency filed actions against a number of companies that process transactions for merchants that accept payments using remotely created checks (RCCs) or remotely created payment orders (RCPOs). In addition to bringing enforcement actions against the merchants for consumer fraud, the FTC filed complaints against the payment processors, in which the agency alleged, generally, that the merchants used deceptive payment methods to extract unauthorized payments from consumers, either at the suggestion of or with the assistance and knowing cooperation of the payment processors. The FTC also claimed that because these types of payment methods do not require the same consumer authorizations required with more mainstream payment methods, such as credit cards, they can be more easily used to defraud consumers.

Although settlements in at least two of these payment processors' actions permanently barred the companies from processing payments for merchants that they "know or should know" are violating the Federal Trade Commission Act or the federal Telemarketing Sales Rule (TSR), the settlements did not include an outright ban on RCCs or RCPOs. The FTC has taken specific aim at these payment methods, however, issuing a Notice of Proposed Rulemaking in May 2013, seeking public comment on proposed amendments to the TSR to prohibit what the agency terms "novel" payment systems. Specifically, the Commission proposes to amend Section 310 of the TSR to prohibit telemarketers from accepting or requesting RCCs, RCPOs, money transfers, and cash reload mechanisms as payment.

The proposed rulemaking highlights those payment systems that the FTC believes can be used in telemarketing scams, focusing particularly on those that the agency believes exploit the use of consumers' bank account and routing numbers to withdraw funds without proper authorization. According to the FTC, "conventional" payment methods – credit cards, debit cards, and other types of electronic fund transfers – are not only processed electronically through networks that can be monitored systematically for fraud, but they are also subject to procedural safeguards and federal regulatory protections. In contrast, the payment methods targeted by the proposed rulemaking are cleared through check clearing and money transfer networks that provide minimal or nonexistent fraud detection and deterrence. These systems are not federally regulated in the same way as conventional payment methods, and in the FTC's view, consumers lack adequate recourse when unauthorized transactions or telemarketing fraud occur. The Commission has also determined that use of these payment methods is itself "an abusive telemarketing act or practice" because they cause or are likely to cause substantial injury to consumers – a harm that is not outweighed by countervailing benefits and that is not reasonably avoidable. Through the proposed rulemaking, the FTC intends to close the regulatory gap in the telemarketing context by prohibiting entirely the use of those payment systems in all inbound and outbound telemarketing transactions.

This proposed rulemaking and the various enforcement actions reflect the FTC's broader campaign against the "gatekeepers" that it believes indirectly facilitate telemarketing fraud. In July 2013 testimony before the U.S. Senate Subcommittee on Consumer Protection, Product Safety, and Insurance, the Commission outlined its strategy for deterring and prosecuting robocall violations, noting that it had

expanded enforcement actions to include charges against payment processors that allegedly knew or consciously avoided knowing key facts about the illegal telemarketing and chose to continue profiting from the allegedly illegal activity by processing payments.

In line with this expanded focus on payment processors, the Commission this month announced another settlement with a payment processor. In this action, the FTC claimed that the processing company used unfair tactics to enable a merchant to engage in a fraudulent "work from home" scheme, including opening and maintaining more than 130 merchant accounts through which the perpetrator of the scheme allegedly charged more than $15 million in unauthorized charges on consumers' debit and credit cards. The agency also alleged that the processor engaged in tactics designed to evade fraud monitoring programs implemented by Visa and MasterCard, including submitting merchant applications that contained false information and distributing transaction volume among numerous merchant accounts (otherwise known as "load balancing") in order to keep those accounts open and to continue to earn fees on those accounts. The complaint against the processor and its principals claimed that the defendants knew or should have known that they were processing unauthorized charges in light of plainly deceptive statements on the merchant websites, notices to the processor that the merchant should be placed in Visa and MasterCard chargeback monitoring programs, and chronically excessive chargeback rates (the percentage of charges that are challenged by consumers, resulting in the charges being reversed). The settlement includes a variety of permanent prohibitions against the company and its principals acting as payment processors.

While the FTC has yet to announce any further action on the proposed rulemaking that would outlaw certain payment methods in the telemarketing arena following the close of the public comment period in August, there can be little doubt that the agency's heightened scrutiny of payment processors will continue.

The FTC is also not the only agency focused on electronic payment system fraud. In Consumer Financial Protection Bureau (CFPB) director Richard Cordray's speech on Nov. 21, 2013, at the annual meeting of The Clearing House Association, which represents the world's largest commercial banks, he opined that payment systems, including credit card payments and automated clearing house (ACH) transactions, had not kept up with developments in the financial landscape, specifically the larger role that nonbank third parties now play in the financial lives of consumers. Noting that other agencies were taking a law enforcement approach to tackling challenges to the safety and security of electronic fund transactions, focusing on cases where they are used for fraudulent or illegal purposes, Cordray suggested that improvements in the system and in the security of transactions should come from a more "holistic" approach addressing the design and function of the system. Cordray's approach would include looking at data and analytics related to the system as a whole to identify trends and potential problems, and then tackling those problems through systemic overhauls, including potential changes to "the law and practice," with the assistance and cooperation of the banking industry.

In light of FTC's increased scrutiny, as well as the CFPB's renewed focus on payment systems, payment processing companies should carefully evaluate whether to allow the use of RCCs, RCPOs, or other similar "novel payment methods" that the FTC claims are used in ways that harm consumers. If processors elect to offer these products, they should implement procedures to monitor potential misuse similar to those used for monitoring conventional payment products, including elevated consumer complaints and/or chargeback rates. If they detect patterns consistent with abusive practices, processors should take prompt steps to investigate and, if necessary, terminate the use of these products by merchants. Processors should consider providing remediation to consumers, in appropriate situations, since the FTC, CFPB, and other regulatory agencies can be expected to look to processors that fail to take these measures to reimburse consumers who have lost money due to fraudulent merchant activities.

For more information about the content of this alert, please contact Michael Mallow or Michael Thurman.

For more information about Loeb & Loeb's Consumer Protection Department, please contact:

ARTHUR W. ADELBERG	AADELBERG@LOEB.COM	202.618.5020
ROBERT M. ANDALMAN	RANDALMAN@LOEB.COM	312.464.3168
MARK D. CAMPBELL	MCAMPBELL@LOEB.COM	310.282.2273
CHRISTIAN D. CARBONE	CCARBONE@LOEB.COM	212.407.4852
TAMARA CARMICHAEL	TCARMICHAEL@LOEB.COM	212.407.4225
DARLENE M. CHO	DCHO@LOEB.COM	310.282.2168
ALBERT M. COHEN	ACOHEN@LOEB.COM	310.282.2228
AURELE A. DANOFF	ADANOFF@LOEB.COM	310.282.2398
PATRICK N. DOWNES	PDOWNES@LOEB.COM	310.282.2352
JESSICA M. HIGASHIYAMA	JHIGASHIYAMA@LOEB.COM	310.282.2072
JENNIFER A. JASON	JJASON@LOEB.COM	310.282.2195
THOMAS P. JIRGAL	TJIRGAL@LOEB.COM	312.464.3150
IEUAN JOLLY	IJOLLY@LOEB.COM	212.407.4810
BENJAMIN KING	BKING@LOEB.COM	310.282.2279
LIVIA M. KISER	LKISER@LOEB.COM	312.464.3170
EDWARD K. LEE	ELEE@LOEB.COM	310.282.2148
RICHARD M. LORENZO	RLORENZO@LOEB.COM	212.407.4288
DAVID G. MALLEN	DMALLEN@LOEB.COM	212.407.4286
MICHAEL MALLOW	MMALLOW@LOEB.COM	310.282.2287
DOUGLAS N. MASTERS	DMASTERS@LOEB.COM	312.464.3144
NERISSA C. MCGINN	NMCGINN@LOEB.COM	312.464.3130
FIONA P. MCKEOWN	FMCKEOWN@LOEB.COM	310.282.2064
DANIEL G. MURPHY	DMURPHY@LOEB.COM	310.282.2215
JAY K. MUSOFF	JMUSOFF@LOEB.COM	212.407.4212
NATHAN J. MUYSKENS	NMUYSKENS@LOEB.COM	202.618.5010
JERRY S. PHILLIPS	JPHILLIPS@LOEB.COM	310.282.2177
RACHEL RAPPAPORT	RRAPPAPORT@LOEB.COM	310.282.2367
CHRISTINE M. REILLY	CREILLY@LOEB.COM	310.282.2361
AMANDA J. SHERMAN	ASHERMAN@LOEB.COM	310.282.2261
MICHAEL B. SHORTNACY	MSHORTNACY@LOEB.COM	310.282.2315
MEREDITH J. SILLER	MSILLER@LOEB.COM	310.282.2294
DENISE A. SMITH-MARS	DMARS@LOEB.COM	310.282.2028
WALTER STEIMEL, JR.	WSTEIMEL@LOEB.COM	202.618.5015
MICHAEL A. THURMAN	MTHURMAN@LOEB.COM	310.282.2122
LAURA A. WYTSMA	LWYTSMA@LOEB.COM	310.282.2251
MICHAEL P. ZWEIG	MZWEIG@LOEB.COM	212.407.4960