

FTC Actions Against Payment Processors Heighten Legal Risks for Service Providers in Privacy Cases

In taking action against two payment processors earlier this month for providing processing services to merchants allegedly engaged in deceptive telemarketing practices, the U.S. Federal Trade Commission demonstrated a broad view of the scope of its authority under the Telemarketing Sales Rule to pursue service providers over the telemarketing practices of their third-party customers or clients. On June 4 and 18, the FTC filed federal lawsuits against Newtek Merchant Solutions and IRN Payment Systems in the U.S. District Court for the Middle District of Florida alleging that the companies provided substantial assistance or support to merchants who the processors allegedly knew or consciously avoided knowing were engaged in deceptive telemarketing schemes. This aggressive enforcement of consumer protection laws against payment processors based on alleged privacy violations by their arms-length customers is of interest to all service providers that do business with consumer-facing clients.

In late 2012 and early 2013, the FTC filed lawsuits against two telemarketing operations, “Treasure Your Success” and “Innovative Wealth Builders,” alleging that the companies engaged in deceptive and abusive telemarketing practices in violation of the Telemarketing Sales Rule (16 C.F.R. § 310) and section 5 of the FTC Act (15 U.S.C. § 45(a)). According to the FTC, the companies cold-called consumers promising to substantially reduce the interest rates on their credit cards and charged customers for such services, but failed to deliver them. In addition, the FTC alleged that Treasure Your Success violated the Do Not Call Registry, did not honor “do not call” requests, and made unwanted robocalls.

In June 2013, the FTC expanded its lawsuits to include as defendants the payment processors that processed the payments made to the telemarketers by consumers, along with the former president of one of the processors. The FTC’s complaints against the payment processors and former president allege that they violated a section of the Telemarketing Sales Rule (16 C.F.R. § 310.3(b)) that prohibits a person from providing “substantial assistance or support to any seller or telemarketer when that person knows or consciously avoids knowing that the seller or telemarketer is engaged in” deceptive telemarketing practices. The FTC’s complaints allege that the processors and former president “knew or consciously avoided knowing” of their clients’ deceptive telemarketing because, according to the FTC, they were aware of high chargeback rates associated with their clients’ transactions and had learned of consumer complaints regarding their clients’ businesses. The complaints further allege that the processors and former president provided “substantial assistance or support” to the telemarketers by providing them with access to the payment card networks and providing related services.

The FTC’s actions in these cases are of concern to all service providers that do business with consumer-facing companies. The suits represent the latest effort by the agency to assert enforcement authority for privacy violations not merely against the companies that commit those violations, but also against companies that provide services to the violators – even if the company is not affiliated with the violator, and even if the violator is not acting as the company’s agent. The FTC’s approach in these cases is reminiscent of other efforts by the agency in recent years to cast a wide regulatory net in privacy and data security cases. The FTC has previously pursued payment processors on similar theories, including a joint action along with state regulators several years ago against payment processor Your Money Access and its officers that resulted in default and stipulated judgments imposing significant injunctive and monetary relief. The FTC also has not limited its broad theories of liability to the payment processing context. In 2011, for instance, the FTC entered into a settlement with several credit report resellers based on allegations that the resellers’ *clients* failed to adequately secure their computer networks.

With its new actions against payment processors Newtek and IRN Payment Systems, the FTC is seeking to revive and expand upon these theories of liability based on logic that could implicate any number of service providers. Indeed, one would think that the very same legal claims could have been leveled by the FTC with equal if not greater force against card brands such as MasterCard, as the FTC's factual allegations in both cases indicate that MasterCard was aware of the telemarketers' fraud yet continued to provide them with access to its payment network. In short, all corporations that provide services to companies that collect or use consumer information should closely watch the FTC's lawsuits against these two payment processors and fully assess the legal risks that might be associated with their business relationships.

For more information regarding the Newtek and IRN Payment Systems actions and their potential impact, please contact a member of our leading privacy and data security team, including [Doug Meal](#), [Mark Szpak](#), [Jim DeGraw](#), and [David McIntosh](#).