WILLIAM H. SORRELL
ATTORNEY GENERAL

SUSANNE R. YOUNG
DEPUTY ATTORNEY GENERAL

WILLIAM E. GRIFFIN
CHIEF ASST. ATTORNEY GENERAL

TEL: (802) 828-3171
FAX: (802) 828-3187
TTY: (802) 828-3665

http://www.atg.state.vt.us

STATE OF VERMONT
OFFICE OF THE ATTORNEY GENERAL
109 STATE STREET
MONTPELIER, VT
05609-1001

August 8, 2013

Federal Trade Commission
Office of the Secretary
Room H-113 (Annex B)
600 Pennsylvania Avenue, NW
Washington, DC 20580

Filed by Mail and Online

Re: Telemarketing Sales Rule, 16 CFR Part 10, Project No. R411001

To Whom It May Concern:

The Offices of Attorney General ("AGOs") of the States of Arizona, Arkansas, Delaware, Hawaii, Illinois, Iowa, Kentucky, Louisiana, Maine, Maryland, Massachusetts, Minnesota, Mississippi, Nevada, New Hampshire, New Mexico, Oregon, Pennsylvania, Rhode Island, Tennessee, Utah, Vermont, and Washington, and of the District of Columbia submit the following comments in response to proposed amendments to the federal Telemarketing Sales Rule ("TSR") set out in a Notice of Proposed Rulemaking ("NPRM") announced by the Federal Trade Commission ("FTC") on May 21, 2013.[1] The Attorneys General are the officials charged with enforcing the laws of the States that protect consumers from unfair and deceptive trade practices.

By way of summary, the AGOs focus their comments on the FTC's proposal to prohibit telemarketers from accepting money transfers and cash reload mechanisms as payment. Specifically, the AGOs recommend that the prohibition extend to transactions proposed by email, which transactions cause as much harm to consumers, if not more, than transactions over the telephone. Indeed, the FTC has an opportunity through this rulemaking to protect thousands of American consumers who otherwise would fall victim to cross-border fraud[2] that uses a combination of emailed offers and money transfers[3] and similar methods of payment.

---

[1] *See* "FTC Seeks Public Comment on Proposal to Ban Payment Methods Favored in Fraudulent Telemarketing Transactions," http://www.ftc.gov/opa/2013/05/tsr.shtm.

[2] The term "cross-border fraud" commonly refers to fraud perpetrated across a national border, but here includes similar types of fraud across state boundaries within the United States.

[3] For the purpose of this discussion, the term "money [or wire] transfer" has the same meaning as "cash-to-cash money transfer" in the NPRM.

I. THE FTC SHOULD PROHIBIT COMMERCIAL EMAIL TRANSACTIONS THAT USE A MONEY TRANSFER AS THE MODE OF PAYMENT

A. The problem of fraud-induced money transfers

For years, the problem of consumer fraud utilizing money transfers as the method of payment—what are sometime called fraud-induced transfers—has caused enormous harm to consumers and evaded a systematic and effective law enforcement solution. This situation has resulted from a perfect storm of factors: the existence of a multitude of scammers in many countries; the use by scammers of difficult-to-trace methods of communication, such as disposable cell phones and emails; a means of payment—money transfers—that can be picked up by a person with a forged ID in many different locations; and the lack of any chargeback or similar rights for consumers. To elaborate on each of these factors:

A multitude of scammers in many countries. Although no precise figures exist, it is clear that there are large numbers of people engaged in defrauding others, including Americans, from locations around the world using money transfers as the mode of payment. Modern methods of communication make it possible to scam consumers from an Internet café in Lagos or a boiler room in Toronto. Among the destinations to which consumers are commonly lured into sending money are Cameroon, Canada, Costa Rica, Ghana, Jamaica, Nigeria, Panama, Peru, Spain, the United Kingdom, and many others.[4] As the FBI has noted, "Large-scale criminal mass-marketing fraud operations are present

---

[4] *See, e.g.,* U.S. Embassy, Yaounde, Cameroon, "Scams Warning, How to Avoid Cameroonian Scams, Frauds Originating From Cameroon," http://yaounde.usembassy.gov/scams_warning.html; IC3, Internet Crime Complaint Center, "2012 Internet Crime Report, 2012 Frequent Reported Internet Crimes, The Grandparent Scam," at 10, http://www.ic3.gov/media/annualreport/2012_IC3Report.pdf; *AP* and *Inside Costa Rica*, "Costa Rica Based Lottery Scammers at it Again," (Sept. 18, 2012), http://insidecostarica.com/2012/09/18/costa-rica-based-lottery-scammers-at-it-again/; Thomas Morton, "Inside the criminal world of Ghana's e-mail scam gangs," *CNN Tech* (Apr. 6, 2011), http://www.cnn.com/2011/TECH/web/04/05/motherboard.ghana.sakawa/index.html; Pia Malbran and Jeff Glor, "Inside the Jamaican Lottery Scam: How U.S. seniors become targets," *CBS News,* (Mar. 12, 2013), http://www.cbsnews.com/8301-505263_162-57573750/inside-the-jamaican-lottery-scam-how-u.s-seniors-become-targets/; *infra* note 24 (Nigeria); Reid Collins, "Guess What Grandpa?!! The Story of a Worldwide Criminal Enterprise," *The American Spectator*, (Jan 16, 2012), http://spectator.org/archives/2012/01/16/guess-what-grandpa (Panama); Laura Gunderson, "Scam alert: Revenue department warns of fraudulent phone calls and emails," *The Oregonian, Oregon Live* (Oct. 31, 2012), http://blog.oregonlive.com/complaintdesk/2012/10/scam_alert_revenue_department.html (Peru); Ellen Roseman, "Woman victimized by Spanish email scam: Don't wire money to someone you know who's in trouble and asks for help unless you verify the person's identity first," *The Star* (Jan. 22, 2012), http://www.thestar.com/business/personal_finance/2012/01/22/woman_victimized_by_spanish_email_scam.html; Bob Greene, "The 'With tears in my eyes' e-mail," *CNN* (Mar. 28, 2010), http://www.cnn.com/2010/OPINION/03/28/greene.email.scam/index.html (United Kingdom).

in multiple countries in most regions of the world."[5] Making matters worse, "[l]aw enforcement intelligence has revealed that a single perpetrator may use hundreds of fraudulent identities and multiple perpetrators may use one common identity, undermining law enforcement efforts to locate perpetrators and intercept fraudulent wire transfers."[6]

Hard-to-trace methods of communication. Mass-fraud, and particularly cross-border, scammers are very hard to find, much less bring to justice. According to the FBI,

> Law enforcement investigations have revealed perpetrators' use of calling cards, cellular phones, and pre-paid SIM cards, the disposable nature of which hinders law enforcement efforts to determine users' identities. West African fraud groups employ free web-based e-mail accounts, frequent multiple Internet cafes, and use Internet phones and other devices that supply instantaneous Internet connections to undermine investigative efforts to trace Internet Protocol addresses. Large scale boiler rooms are investing in sophisticated computer systems and storing servers in other countries, trusting that the complexity of cross-border cases deters law enforcement investigation. Recent investigations indicate that fraudsters manipulate the caller identification features of Internet-based technology, including VoIP and platform numbers, to create the appearance of operating within victims' cities or countries rather than from overseas locations.[7]

Flexible pickup of funds. Money transfers in particular offer advantages to scammers on the receiving end of the payment conduit. For instance, "West African fraud groups commonly request payment via wire transfers, which produce minimal documentation, can often be collected with forged identification, and may be rapidly retrieved from nearly any location."[8] Indeed, wire transfers can be picked up almost

---

[5] Federal Bureau of Investigation, *Mass-Marketing Fraud: A Threat Assessment, International Mass-Marketing Fraud Working Group* (June 2010), http://www.fbi.gov/stats-services/publications/mass-marketing-fraud-threat-assessment (hereinafter "*FBI*").

[6] *FBI.* With respect to the protean yet shadowy nature of West African cross-border fraud, the FBI report states, "West African criminal enterprises are highly adaptive and opportunistic, perpetrating nearly every type of mass-marketing fraud, including the ubiquitous 419 schemes as well as lottery, loan, investment, and work-at-home schemes. The groups often share successful fraud techniques with and provide assistance to other cells, a practice that may result in the commission of nearly identical schemes by multiple groups acting in relative independence of one another. They frequently employ individuals with specialized skills to impersonate attorneys, government officials, and bankers; design websites; forge checks; translate documents into foreign languages; collect wire transfers; and process incoming and outgoing mail."

[7] *Id.*

[8] *Id.*

immediately in any of hundreds or thousands of locations with minimal scrutiny, and thus afford scammers an ideal conduit for the flow of consumer monies.[9]

Absence of chargeback rights. Compounding the difficulty for consumers is the fact that unlike with fraudulent credit card payments or unauthorized bank debits, senders of money transfers have no established right to a refund once their transfer has been picked up, regardless of how fraudulent the conduct of the receiver was in inducing the transaction.[10] The FTC makes this point in its NPRM, noting that federal and state laws "fail to provide consumers with the means to recoup their money once they discover the fraud."[11]

Scams involving money transfers come in a number of forms, the details of which can vary over time. However, some of the predominant types of scams include the following:

"The grandparent scam." An older consumer receives a telephone call from a person who sounds like her grandson; he says he is in trouble and needs money wired to him immediately. Often the story is that the grandson has been in a car accident, or has been arrested, in Canada or Mexico, and needs funds for medical care, bail, or car repairs; the caller will often ask that "his parents" not be contacted. However, the call is not from the consumer's grandson; it is from a scammer; and once the grandparent sends money, the scammer may call back and ask for more.

Lottery scams. A consumer receives a call stating that he has won a lottery or sweepstakes or qualified for a government grant, but must send money, usually by money transfer, to cover "fees," "taxes," or other charges. In fact, the lottery/sweepstakes/grant does not exist, the consumer has not won anything, and the money is being sent to a scammer.

---

[9] Western Union has over 489,000 agent locations. http://www.westernunion.com/send-money-in-person. Money can also be sent online "24/7" and picked up in cash, or, in some countries, deposited into a bank account or mobile wallet. http://www.westernunion.com/us/send-money/send-money-online.page?prop14=us_hmp_sendmoney_smon_learnmore&evar23=us_hmp_sendmoney_smonlearnmore. MoneyGram has over 244,000 agents. http://www.moneygram.com/MGICorp/campaigns/moneytransfer/index.htm.

[10] Western Union states, "You can cancel or stop a regular money transfer as long as it the receiver [sic] hasn't yet picked up the money. This may not be possible on a money order, bill payment or prepaid money transfer." https://thewesternunion.custhelp.com/app/answers/detail/a_id/118/session/L3RpbWUvMTM3MDM3MzE1My9zaWQvUG9tOVpWcmw%3D. Similarly, according to MoneyGram, "You cannot cancel a Transfer or request a refund after the Receive Amount has been disbursed. Except as required by law, MoneyGram will not be responsible or liable to you or any other person for its failure for any reason to cancel a Transfer." https://www.moneygram.com/wps/mgo/jsps/sendmoney/includes/terms.jsp?standalone=1.

[11] *See* NPRM at 47.

"Nigerian scams." A consumer receives an email stating that a wealthy person has died—often in Africa—and that someone in the U.S. is needed to safeguard the deceased's money in a bank account. However, there is no such wealthy person; it is just a lie to lure the consumer to wire money to the scammer, for "fees," "taxes," or other charges.

"Romance scams." An individual is contacted by a stranger, often claiming to be a young person of the opposite sex. The stranger expresses an interest in being a "pen pal" and perhaps talks about wanting to come to America. Then there is a heartfelt request for money to be wired—to replace a lost airplane ticket, to pay medical bills after a sudden accident, or for some other reason. It is all a scam.

"Counterfeit check scams." A consumer who is selling an item online or through the newspaper receives a check for *more* than the asking price. Even if the funds, once deposited, are treated by the bank as "available" for withdrawal, the check is still counterfeit—a fact that is not known for some days or weeks. By then, the consumer has wired a refund to the scammer for the excess payment. (The use of the counterfeit checks overlaps with other scams, including lotteries and "secret shopper" scams. In all of these cases, the consumer receives an overpayment and then is asked to send money back.)[12]

As for the overall extent of the problem for American consumers, that cannot be known with precision, but it is clearly very substantial. There are "strong indications" that losses to global mass-marketing fraud is in the tens of billions of dollars per year.[13] The scope of this type of fraud is also reflected in surveys conducted of money transferors selected at random (not complainants). A multistate survey conducted in 2003 showed, strikingly, that over 29 percent of transfers and 58 percent of transferred dollars from the United States to Canada through Western Union in 2002 were the result of fraud (a number that is believed to have been "artificially" low because the sampled transfers included dollar amounts down to $300).[14] The comparable figure for transfers to Canada of $1,000 or more through MoneyGram over a four-month period in 2007 was an astonishing 79 percent, according to the FTC.[15]

---

[12] All of these scams are described on the FTC's website. *See* http://www.consumer.ftc.gov/articles/0204-family-emergency-scams; http://www.consumer.ftc.gov/articles/0086-international-lottery-scams; http://www.consumer.ftc.gov/articles/0002l-nigerian-email-scam; http://www.consumer.ftc.gov/articles/0004-online-dating-scams; and http://www.consumer.ftc.gov/articles/0159-fake-checks. *See also* David N. Kirkman, "Fraud, Vulnerability and Aging: When Criminals Gang Up on Mom and Dad," 17th Annual Elder Law Symposium, N.C. Bar Association (Feb. 22, 2013) (describing current scams targeting the elderly, including cross-border telemarketing and Internet scams using money transfers).

[13] *FBI.*

[14] "Western Union Enters into Settlement with Attorneys General" (Nov. 14, 2005), http://www.atg.state.vt.us/news/western-union-enters-into-settlement-with-attorneys-general.php.

[15] *See FTC v. MoneyGram International, Inc.*, No. 1:09-cv-06576 (N.D. Ill., Oct. 19, 2009) (Complaint for Injunctive and Other Equitable Relief), ¶ 27, http://www.ftc.gov/os/caselist/0623187/091020moneygramcmpt.pdf.

B. The use of email in connection with fraud-induced money transfers.

The AGOs strongly support the FTC's proposal to prohibit telemarketing that calls for payment by money transfer. Certain categories of scam do utilize this telemarketing-plus-money-transfer model. For example, grandparent scams typically begin with a telephone call to an older consumer from someone claiming to be the consumer's grandchild, who asks for money—often thousands of dollars—to bail him out of jail, repair a damaged car, or deal with some other supposed emergency. Some lottery scams also use an initial telephone contact.[16]

However, other types of scam employ *email* communications to target consumers. These include "Nigerian" or "419" scams,[17] romance scams,[18] and counterfeit-check scams.[19] These communications involve relatively sophisticated techniques and high numbers of contacts. As the FBI describes the situation,

> Law enforcement intelligence reveals perpetrators' increasing use of e-mail spiders, which crawl through websites, message boards, and other online forums to harvest e-mail addresses for subsequent solicitation via spam e-mail. Once the e-mail addresses have been collected, fraudsters often employ botnets—networks of computers infected with malicious code and programmed to follow the directions of a common command-and-control server—to facilitate the simultaneous distribution of thousands of spam e-mails. Perpetrators also pose as buyers and sellers on online auction websites, upload fake jobs to employment websites, and create bogus user accounts on social networking and dating websites to target new victims and initiate fraud schemes under the guise of legitimacy. While the majority of recipients delete or ignore Internet-based solicitations, their widespread distribution ensures that some recipients will believe the messages to be credible and respond accordingly. In addition, some recipients may perceive the e-mail solicitations to be fraudulent but respond anyway, thereby validating their e-mail addresses to the fraudsters and increasing the likelihood of future fraudulent solicitations."[20]

---

[16] *See, e.g.*, AARP, "Scammers Lurk Behind Area Code 876: Older residents should beware of threatening con artists using Jamaican numbers" (Sept. 2012), http://www.aarp.org/money/scams-fraud/info-09-2012/beware-area-code-876-nh1788.html.

[17] *See, e.g.*, FBI, "Common Fraud Schemes, Nigerian Letter or "419' Fraud," http://www.fbi.gov/scams-safety/fraud.

[18] IC3, Internet Crime Complaint Center, "2012 Internet Crime Report, Romance Scams," http://www.ic3.gov/media/annualreport/2012_IC3Report.pdf, at 16.

[19] IC3, Internet Crime Complaint Center, "Intelligence Note: U.S. Law Firms Continue to be the Target of a Counterfeit Check Scheme" (Mar. 12, 2012), http://www.ic3.gov/media/2012/120312.aspx.

[20] *FBI.*

Significantly, there is reason to believe that money transfers induced by fraudulent email exceed money transfers induced by fraudulent telemarketing by a wide margin. According to data in the FTC's Consumer Sentinel national complaint database, for the period January 1, 2011, through June 3, 2013, the number of complaints involving "wire transfers" where the method of contact was "telephone" was 26,379; monetary losses reported in those complaints totaled $188,963,368. The comparable figures for complaints involving money transfers where the method of contact was "email" were 67,217 and $596,315,020—respectively *over two and one-half and three times as high* as the telephone-related figures.[21]

This is not to deny the magnitude of the problem of fraudulent telemarketing that utilizes money transfers, but rather to stress the equivalent or greater magnitude of the problem of fraudulent electronic communication that use the same payment method.[22]

From the scammer's point of view, contacting potential victims by email has certain advantages. The technology allows a scammer to contact huge numbers of consumers rapidly and at minimal cost.[23] Emails also allow for a high level of anonymity, concealing the origin of the messages, masking cues (such as manner of speaking) as to the sender's identity and origin, and allowing scammers to convincingly pretend that they are someone they are not—such as an older man representing himself to be a younger woman as part of a romance scam.

---

[21] In Consumer Sentinel, the payment method "Wire Transfer" includes Bank Transfer Other, Wire Transfer—MoneyGram, Wire Transfer—Western Union, and Wire Transfer—Other; initial contact "Telephone" includes Mobile—Text/Email/IM, Phone, Phone Call—Landline; Phone Call—Mobile/Cell, and Wireless; and initial contact "Email" includes Email and Internet/Mail. The data cited in the text and these definitions are based on information obtained from the FTC and the Consumer Sentinel Network on June 7, 2013.

[22] For the period May 29, 2012 through May 29, 2013, 58.5 percent of all complaints to the National Consumers League ("NCL") involved money transfers as the payment method. Email from NCL to Vermont Attorney General's Office (June 11, 2013). Likewise, according to complaints filed with the FTC in the calendar years 2010 through 2012, the most common method of scammers' contacting consumers was email (43, 42 and 38 percent, respectively), followed by telephone (20, 29 and 34 percent, respectively), and additional contacts over the Internet (11, 13 and 12 percent, respectively). FTC, *Consumer Sentinel Network Data Book for January-December 2012*, at 9 (Feb. 2013), http://www.ftc.gov/sentinel/reports/sentinel-annual-reports/sentinel-cy2012.pdf.

[23] *See* Robyn Dixon, "Nigerian Cyber Scammers: To the cyber scammers in Nigeria who trawl for victims on the Internet, Americans are easy targets. But one thief had second thoughts," *L.A. Times* (Oct. 20, 2005), http://www.latimes.com/technology/la-fg-scammers20oct20,0,4094532,full.story ("He sent 500 e-mails a day and usually received about seven replies."). *Cf.* "EFCC Bust Nigerian 419 Scammers," http://video.onlinenigeria.com/Drama/adHG.asp?blurb=1345 (video showing a raid on an Internet café by a unit of Nigeria's Economic and Financial Crimes Commission and confiscation of computers and other evidence, including lists of email addresses used to send mass scam messages to Westerners).

The impact of email-initiated fraud-induced money transfers can be devastating on consumers. Among countless accounts of fraud, there are these:

- M.B., age 79, a resident of Vermont, met "Alex" through email contacts she received from an online religious dating website. During their online email and instant message conversations, Alex expressed to M.B. that his best friend's wife had cancer and that he was raising money to fund research of cancer-fighting herbs. For the next four months, Alex sent specific instructions to M.B. on how to discreetly send money to Ghana by splitting wire transfers into $2,000 increments and to use various wire transfer locations. By the time anyone in M.B.'s family noticed what she was doing, almost $44,000 had been wired to the scammer.

- G.R., a self-employed resident of Washington struggling to support herself, posted her resume on several websites. Scammers emailed her to offer a position as "operations manager" responsible for "processing customers' payments"; she was also instructed to complete an employment agreement and provide her bank account information for payroll purposes. She received checks totaling over $16,000, a sum that, as instructed by the scammers, she deposited in her bank account and then withdrew and wired to four individuals in Russia. Her bank soon informed her that it had frozen her account because the deposited checks did not clear, and that she was solely responsible for repaying the full amount.

- G.H., a 57-year-old divorced and unemployed resident of Illinois, began an online relationship with Robert through a dating website. G.H. told Robert she needed a job, and Robert promised he had work for her in his business as an antique dealer. Soon after, Robert said he was traveling in Nigeria for work, and that his wallet had been stolen. He asked G.H. if she could send money to help him get home. She responded and wired a little over $1,000 to Robert as instructed. This began a series of hard luck stories and requests for additional money from Robert. G.H. sent a total of $23,800 to Robert in multiple wire transfers of approximately $1,000 each before she realized she was being scammed.

- B.A., a resident of Ohio, was looking for employment online and received an email offer supposedly from a pharmaceutical company supplier. The email stated that the consumer would be sent a check, which he was to deposit and draw on to send money by wire transfer to pharmaceutical company representatives. The consumer would then receive packages of supplies and another check for shipping costs; and he would be paid $500 a week. The consumer received and deposited a $6,850 check, and wired three payments of $1,950 each. A week later, the consumer's bank told him that the deposited checks were fraudulent and demanded that he pay back the money he withdrew.

C. Recommendation: The prohibition on telemarketing using money transfers should extend to commercial email communications using money transfers.

If the FTC is going to amend the TSR to prohibit telemarketing transactions in which the consumer's payment is sent by money transfer—and it should do so—then that prohibition should also extend to commercial *emails* sent to consumers that utilize a money transfer as the mode of payment. As noted above, if anything, the impact on U.S. consumers of money transfers induced by fraudulent emails is greater than the impact of money transfers induced by fraudulent telemarketing. Including emails used as the method of contact in these situations, alongside telemarketing, can be expected to deal a substantial blow to cross-border fraud that has up until now eluded an effective solution.

The AGOs understand that the FTC's authority to amend the TSR in this way may be constrained by the terms of the Telemarketing Consumer Fraud and Abuse Prevention Act, which required the Commission to prescribe rules focused on consumer fraud through telemarketing.[24] However, there are other avenues available to the Commission to avoid creating a major loophole in the fabric of protection afforded by the Rule, including promulgating a trade regulation rule under the Federal Trade Commission Act,[25] clarifying its position through litigation, or including a comment in its discussion of adopted amendments to the TSR—any of which could in turn empower States that have consumer protection statutes that look to federal precedent for guidance.[26]

II. THE FTC SHOULD CLARIFY THAT A MONEY TRANSFER COMPANY'S FAILURE TO MAKE REASONABLE INQUIRY INTO WHETHER A PROHIBITED METHOD WAS USED TO INDUCE A CONSUMER TO SEND A MONEY TRANSFER IS UNLAWFUL.

The FTC's proposal to ban telemarketing that utilizes a money transfer as the method of payment is laudable, as would be extending that ban to email. Nonetheless, the reality is that any legal prohibition directed solely to the *scammers* is itself likely to have little impact on the incidence of fraud-induced transfers. The people who engage in this type of fraud are already violating the law by offering non-existent lottery winnings, false "grandchild" claims, illusory romances, and the like. In many cases, their conduct is criminal; they cannot be expected to care about complying with the civil TSR. Nor, as noted above, can they be easily found and brought to justice.

---

[24] *See* 15 U.S.C. § 6102(a)(1) (requiring the FTC to prescribe rules prohibiting "deceptive telemarketing acts or practices and other abusive telemarketing acts or practices").

[25] *See* 15 U.S.C. § 57a.

[26] *See, e.g.*, 9 Vt. Stat. Ann. § 2453(b) ("It is the intent of the legislature that in construing subsection (a) of this section [prohibiting unfair and deceptive acts and practices in commerce], the courts of this state will be guided by the construction of similar terms contained in Section 5(a)(1) of the Federal Trade Commission Act as from time to time amended by the Federal Trade Commission and the courts of the United States.").

If the FTC is to reduce the incidence of cross-border and similar fraud, it needs to make clear the legal responsibility, and liability, of the entities that *control the method of payment*. These are the money transfer companies, without whose payment systems much of the fraud at issue would not be possible. As noted earlier, there is already precedent for taking legal action, at the state and/or federal level, against such businesses for failing to provide adequate protection from fraud for their customers. It is now appropriate, indeed critical, for the FTC to clarify those companies' responsibility for making reasonable inquiry into whether consumers who propose to wire money are doing so in response to a prohibited communication.

Under the TSR, it is a deceptive telemarketing act or practice and a violation of the Rule for a person to "provide 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 any act or practice that violates ... § 310.4 of [the] Rule."[27] There is no question that the money transfer companies provide "substantial assistance or support" to those who use deception to induce consumers to wire them money. If the FTC amends § 310.4 to prohibit telemarketers from accepting payment by money transfers, it is only reasonable to expect the money transfer companies to inquire of their customers as to whether this prohibition is being violated, and to consider failure to inquire a third-party violation of § 310.3(b). Indeed, the FTC has already taken a similar position in *FTC v. MoneyGram International, Inc.*[28] The FTC is also urged to extend this approach to encompass emails utilizing money transfers as the mode of payment.

---

[27] 16 C.F.R. § 310.3(b) (emphasis added).

[28] The FTC's Complaint in that case states, in pertinent part,

> **VIOLATIONS OF THE TELEMARKETING SALES RULE**
> **COUNT II**
> ***Assisting and Facilitating Telemarketing Sales Rule Violations***
>
> 91. In numerous instances, in the course of processing money transfers sent by U.S. consumers, Defendant or its agents have provided substantial assistance or support to sellers or telemarketers who Defendant or its agents knew or consciously avoided knowing:
>
> a. Induced consumers to pay for goods and services through the use of false or misleading statements, including, without limitation, the statement that the consumer has won and will receive a large cash award if the consumer pays a requested fee or fees, in violation of Section 310.3(a)(4) of the Telemarketing Sales Rule, 16 C.F.R. § 310.3(a)(4); and
>
> b. Requested or received payment of a fee or consideration in advance of consumers obtaining a loan when the seller or telemarketer has guaranteed or represented a high likelihood of success in obtaining or arranging a loan for a person in violation of Section 310.4(a)(4) of the Telemarketing Sales Rule.
>
> 92. Defendant's acts or practices alleged in Paragraph 91 constitute deceptive telemarketing acts or practices in violation of Section 310.3(b) of the Telemarketing Sales Rule and Section 5(a) of the FTC Act, 15 U.S.C. § 45(a).

III. UNDER THE TSR, CASH RELOAD MECHANISMS SHOULD BE TREATED THE SAME AS MONEY TRANSFERS.

In recent years, the States have seen increasing use of "cash reload" payment mechanisms to transfer funds as part of scams. Many work-at-home, advance-fee loan, and sweepstakes scam victims are now directed to make payments utilizing this system. As with money transfers, cash reloads are an especially risky means of payment; once the consumer (victim) provides the scammer with the account number of the cash reload "pack," the scammer has instant access to the funds in that pack. Because of their increasing availability, ease of use, and minimal oversight by regulatory authorities, cash reload systems are an attractive payment vehicle for scammers. The AGOs support amendments to the TSR that would expressly prohibit telemarketers from accepting cash reloads as a means of payment, and further recommend, consistent with their comments on money transfers, that the ban be extended to include offers via email.

IV. THE AGOs SUPPORT THE PROPOSED BAN ON REMOTELY CREATED CHECKS.

By letter dated May 3, 2005, the Attorneys General of 34 States, the District of Columbia, and American Samoa took the position that remotely created checks (also called demand drafts) are "frequently used to perpetrate fraud on consumers," and urged the Board of Governors of the Federal Reserve System to eliminate such checks in favor of electronic funds transfers that can serve the same payment function.[29] The letter noted several features of remotely created checks that make them "an ideal method of siphoning money from consumers": lack of consumer awareness of how strangers can debit their bank accounts without authorization; the ease with which remotely created checks can be created, using freely-available software and ink; the fact that a scammer, or his processor, does not need special access to the banking system but can simply deposit the drafts to his own bank account; the difficulty, if not impossibility, of tracking remotely created checks; and the hurdles that consumers often encounter in trying to obtain a recredit to their bank account when—if at all—they discover an unauthorized debit (hurdles such as unclear or restrictive time frames for requesting a return, uninformed or hostile bank tellers, and the lack of incentives to the receiving bank's initiating the return process).

Consistent with the views expressed in 2005, the AGOs support the proposed ban on the acceptance of remotely created checks by sellers and telemarketers.

FTC v. MoneyGram International, Inc., No. 1:09-cv-06576 (N.D. Ill., Oct. 19, 2009) (Complaint for Injunctive and Other Equitable Relief), http://www.ftc.gov/os/caselist/0623187/091020 moneygramcmpt.pdf.

[29] In the alternative, the signatories to the letter stated that "if demand drafts are to continue to be used, the proposed originating-bank warranty of authorization should augment, not supplant, the existing receiving bank warranty; and ... demand drafts should be mandatorily marked as such."

V. THE AGOs SUPPORT THE OTHER PROPOSED AMENDMENTS TO THE TSR.

The AGOs also express their support for the other proposed amendments to the TSR, including broadening the ban on telemarketing recovery services to include losses incurred in any medium, and requiring that the recording of a consumer's express verifiable authorization include a description of the goods or services being purchased.

The AGOs thank the Federal Trade Commission for its consideration of these comments.

Sincerely,

Elliot Burg
Senior Assistant Attorney General