

Indeed, trading in unencrypted consumer account numbers has been uniformly condemned by virtually all parties who participated in this rulemaking proceeding. Although there was substantial debate regarding the Commission's proposal for a blanket prohibition on the transfer or receipt of consumers' billing information (*i.e.*, "preacquired account information"),⁴¹⁶ there was no disagreement among commenters and forum participants about the notion that trafficking in lists of consumer account numbers was improper, in many cases illegal, and should be a violation of the Rule.⁴¹⁷ As ERA explained during the forum:

[I]f there is a transfer of consumer information without knowledge of and prior to the consumers' consent, which would encompass, for example, your scenario where a list is compiled and a marketer [sold] its list with its credit card numbers to another marketer without telling the consumers on that list that they sold the list of account numbers, I think everyone at this table would agree . . . that this is a violation. . . . We've said in our comments that we would agree to a ban on that. Legitimate marketers don't do that. They don't sell consumer credit card numbers for money.⁴¹⁸

Given that there is no legitimate reason to purchase unencrypted credit card numbers, the Commission believes there is a strong likelihood that telemarketers who engage in this practice will misuse the information in a manner that results in unauthorized charges to consumers. This conclusion is consistent with the Commission's law enforcement experience.⁴¹⁹ Consumers

they should not get a credit card or other account number except from the consumer who chooses to deal with them. . . . This should include not SELLING (not just sharing as stated in our newspaper article) these numbers."'); Anonymous (Msg. 3457) ("This is not what any reasonable person would consider "public information." . . . Why would ANYONE consider this information that they can "share" without the customer's express permission?").

⁴¹⁶ Over 50 of the major organizational commenters addressed the issue of preacquired account telemarketing, as did over 200 consumer commenters. In addition, a session of the June 2002 Forum was dedicated to the topic, and generated extensive discussion. See June 2002 Tr. II at 116-212.

⁴¹⁷ See, *e.g.*, ERA/PMA-Supp. at 14-15; PMA-NPRM at 14; June 2002 Tr. II at 183 (ERA). See also ATA-Supp. at 6; NCTA-NPRM at 12 ("[T]he trafficking of customer account information by unscrupulous telemarketers is a legitimate concern."). Also, the GLBA prohibits this practice on the part of financial institutions. 15 U.S.C. 6802(d); and see, *e.g.* 12 CFR 313.12.

⁴¹⁸ June 2002 Tr. II at 183.

⁴¹⁹ See, *e.g.*, *FTC v. J.K. Publ'ns, Inc.*, 99 F. Supp. 2d 1176 (C.D. Cal. 2000) (in which, outside the telemarketing context, defendant purchased unencrypted lists of consumer account numbers, which it used to charge consumers, purportedly for visits to adult websites, despite the fact that many of those charged did not even own computers). In

cannot avoid the injury because they likely are unaware that their credit card numbers have been purchased and that a telemarketer possesses that information when they receive a telemarketing call. In addition, there is no evidence on the record of any countervailing benefits to consumers or competition by trafficking in lists of account numbers. As a result, the Commission concludes that the practice of selling unencrypted lists of credit card numbers is likely to cause substantial and unavoidable consumer injury in the form of unauthorized charges without any countervailing benefits. Thus, the Commission has determined to add Section 310.4(a)(5). This provision is consistent with the basic prohibition in the GLBA, and in essence, extends the ban on this practice beyond financial institutions and ensures that all sellers and telemarketers subject to the TSR are prohibited from this practice.

The prohibition in § 310.4(a)(5) is not limited to compilation and disclosure of lists of account numbers. Rather, any disclosure (or receipt) of unencrypted account information violates the Rule, unless the disclosure is for purposes of processing a payment for a transaction to which the consumer has consented after receiving all disclosures and other protections of the Rule. A seller or telemarketer could not, for example, provide or receive account numbers one at a time in order to circumvent this provision. Nor could a telemarketer obtain account information from consumers on behalf of one seller, and then retain it for sale or disclosure to another seller in another telemarketing campaign.⁴²⁰

In addition, given the evidence that preacquired account telemarketing involving encrypted account information can result in unauthorized charges (as discussed in more detail below), the Commission believes that there is an even greater likelihood of consumer injury when telemarketers have purchased consumers' actual credit card numbers before contacting consumers about an offer.

⁴²⁰ See, *e.g.*, *FTC v. Capital Club*, No. 94-6335 (D.N.J. 1994). According to the FTC complaint in that case, two companies, National Media and Media Arts, which marketed products through infomercials, allegedly sold or rented their customer lists to third-party service companies that sold products and services such as memberships in shopping and travel clubs. The lists contained customers' names, addresses, and telephone numbers, as well as their credit-card types, account numbers and expiration dates. The lists were provided to the service companies without the customers' knowledge or authorization. Some of the Capital Club defendants' roles included maintaining the lists, marketing them to the service companies, and conducting telemarketing calls on behalf of the service companies, according to the complaint. Industry representatives at the June 2002 Forum registered agreement that the Capital Club scenario would run afoul of a ban on trafficking in consumer account information. See June 2002 Tr.

By "unencrypted," the Commission means the actual account number, or lists of actual account numbers, or encrypted information with a key to unencrypt the data.⁴²¹ "Consideration" is not limited to cash payment for a list of account numbers. "Consideration" can take a variety of forms, including receiving a percentage of every "sale" using the unencrypted account information.

This provision allows processing a properly obtained payment for goods or services pursuant to a transaction. In addition, pursuant to the USA PATRIOT Act's expansion of the TSR to cover charitable solicitations, the provision also allows for the disclosure or receipt of a donor's account number to process a payment for a charitable contribution pursuant to a transaction. By "transaction," the Commission means a telemarketing transaction that complies with all applicable sections of the Rule, including new § 310.4(a)(6), discussed below, which prohibits any seller or telemarketer from causing a charge to be placed against a customer's or donor's account without that customer's or donor's express informed consent to the charge.⁴²²

§ 310.4(a)(6) — Causing a charge to be submitted for payment without the consumer's express informed consent

In the NPRM, the Commission proposed a prohibition on "receiving from any person other than the consumer or donor for use in telemarketing any consumer's or donor's billing information, or disclosing any consumer's or donor's billing information to any person for use in telemarketing."⁴²³ This proposed provision was prompted by extensive comments during the Rule Review concerning the severity and the scope of harm to consumers related to

II at 193 (ERA) ("[T]hat's exactly the scenario that we're talking about that would be prohibited because when that third-party telemarketer retained that account information, it did so as an agent for the seller, so it was not that telemarketer's account information to begin with. They were capturing that for the seller on whose behalf that call was made, so if that telemarketer were then to call a consumer without knowledge and prior consent and use that credit card information again, that would be the kind of a transfer prior to and without consumer consent that we're talking about.")

⁴²¹ This, too, is consistent with the financial privacy regulations issued pursuant to the GLBA. See 12 CFR 313.12(c)(1) ("An account number, or similar form of access number or access code, does not include a number or code in an encrypted form, as long as you do not provide the recipient with a means to decode the number or code.") (emphasis added).

⁴²² See amended Rule § 310.4(a)(6) and discussion of that provision, below.

⁴²³ Proposed Rule § 310.4(a)(5), 67 FR at 4543.