



November 13, 2014

By Electronic Delivery

Office of the Secretary, Suite CC-5610 (Annex B)
Federal Trade Commission
600 Pennsylvania Avenue NW.
Washington, DC 20580

Re: Telemarketing Sales Rule Review, 16 CFR Part 310, Project No. R411001

Ladies and Gentlemen:

This letter is submitted by Visa Inc. (“Visa”) in response to the request for comment by the Federal Trade Commission (“FTC” or “Commission”) in connection with the Commission’s review of its Telemarketing Sales Rule (“TSR” or “Rule”).¹ As part of the FTC’s ongoing efforts to examine the efficacy, costs, and benefits of its rules, the Commission is reviewing the TSR and seeking comment on a number of issues, including whether the Rule should be updated to further address the use of preacquired account information in telemarketing in light of changes in the legal landscape since these provisions were adopted in 2003.

Visa plays a leading role in advancing payment products and technologies worldwide to benefit hundreds of millions of consumers. Visa does not itself issue payment cards to consumers, but rather it operates the network supporting Visa-branded credit, debit and prepaid card products designed by issuing banks to enable their customers to make purchases at merchants and retailers globally and receive funds in a convenient, secure, and reliable manner. Protecting cardholders and the integrity of the electronic payments system is therefore paramount among Visa’s priorities to ensure that when consumers use their payment cards, they have confidence that they will only be charged for the products and services they intend to purchase.

Visa appreciates the Commission’s invitation to interested parties to comment on the continuing need for the TSR and possible improvements to the Rule in light of changes in the marketplace since the Rule was last revised.

Visa Supports the FTC’s Rule Review Efforts

Visa commends the FTC on its ongoing efforts to periodically review and update its rules and guides to assess their effectiveness and their associated costs and benefits for consumers and businesses alike as new payment technologies and capabilities are introduced

¹ 79 Fed. Reg. 46732 (August 11, 2014).

and consumer payment preferences evolve in response to these new innovations. These efforts can help to identify outdated regulatory provisions that are in need of adjustment or deletion as well as changes to the marketplace that warrant further clarification as to how the TSR should be applied. The FTC's commitment to reviewing the TSR is particularly timely to ensure that existing consumer protections keep pace as commerce and payments increasingly become digitized.

Visa's Ongoing Initiatives to Protect Cardholder Security and Confidence in the Payment System

Visa has long recognized the critical importance of protecting cardholders and the integrity of the payment system regardless of the payments environment or the channel in which the transaction takes place. For example, as consumers increasingly move away from face-to-face retail environments and engage in online commerce, Visa has enhanced its fraud screening technologies and introduced new tools and services, including Verified by Visa and Visa Checkout, to better protect merchants and cardholders in the online environment. In the unfortunate event that unauthorized transactions do occur on a Visa credit, debit, or prepaid card account, cardholders are protected by Visa's Zero Liability Policy, in addition to their existing dispute resolution rights under federal law. In October 2014, Visa announced an investment of more than \$20 million to educate consumers and merchants on payment security, in addition to launching a 20-city national public service campaign.

Visa has also launched Visa Token Service to enable financial institutions to replace traditional payment card account numbers with digital account numbers or "tokens" for use when consumers engage in online and mobile purchases. In addition to removing sensitive account credentials from the payments environment, tokens can also be restricted for use with a specific merchant, mobile device, transaction or category of transactions to further enhance cardholder security and confidence in mobile transactions. This investment in tokenization coupled with EMV chip technology and dynamic forms of authentication reflect Visa's commitment to ensuring that consumers can continue to pay with confidence in a safe and secure manner while reducing the threat of sensitive personal account data being compromised.

The TSR Should be Updated to Protect Consumers from the Use of Preacquired Account Information by Third Parties

The Telemarketing and Consumer Fraud and Abuse Prevention Act of 1994 was enacted to target deceptive and abusive telemarketing practices, and specifically directed the FTC to issue a rule defining and prohibiting deceptive and abusive telemarketing acts or practices.² Pursuant to that directive, the FTC promulgated the TSR in 1995 and has since amended the Rule on several occasions to address additional telemarketing practices. Among other things, the TSR sets forth mechanisms to protect consumers from unauthorized charges or debits to their financial account, such as a requirement for telemarketers to obtain

² 15 U.S.C. 6101-6108.

a consumer's "express informed consent" before the consumer may be billed to a particular account or a payment is collected. Currently, the TSR restricts, but does not prohibit, the use of preacquired account information in telemarketing, even if consumer payment information could be used to place a charge against the consumer's account for purchases beyond the transaction for which the information was originally obtained.

As the Commission notes, there have been significant changes in the legal landscape since the FTC amended the TSR in 2003 to address the use of preacquired account information in telemarketing. In December 2010, Congress enacted the Restore Online Shoppers' Confidence Act ("ROSCA"),³ to prevent businesses from billing online consumers' credit and debit cards for items they have not ordered. ROSCA's passage followed a lengthy Senate investigation into so-called "data pass" marketing practices in which online third-party marketers billed consumers without the consumers' knowledge or consent for additional goods or services (e.g., club memberships) using previously acquired payment information from a prior purchase. Under ROSCA, an "initial merchant" is prohibited from disclosing a consumer's billing information to any "post-transaction third-party seller" for the purpose of charging the consumer's account. In addition, the third-party seller must obtain separate consent and full payment information directly from the consumer before charging a transaction to the consumer's account.⁴

The operating rules of the three major payment brands are consistent with ROSCA in prohibiting the disclosure, exchange, or use of preacquired credit card account information by and among their merchants. For example, the Visa Product and Service Rules (formerly the Visa Operating Regulations) have long prohibited acquirers and merchants from disclosing a cardholder's credit or debit card account number and other Visa transaction information to any entity that is not directly involved in completing or processing the transaction.⁵ To curb "data pass" practices and provide a clear signal to cardholders when a second purchase is being initiated to their account, in April 2010 Visa adopted additional protections which require merchants to prompt consumers to re-enter their card information before a consumer may accept a subsequent offer from a third-party merchant.⁶ The adoption of this requirement followed Visa's launch of a program with the FTC and the Better Business Bureau in December 2009 to educate consumers on deceptive marketing practices.

These measures reflect Visa's ongoing efforts and commitment to protect consumer security and confidence in the payments system and our recognition of the harmful effects that deceptive marketing practices can have in undermining its efficiency, reliability and security. Visa urges the FTC to explore further revisions to the TSR consistent with

³ Pub. L. 111-345, 124 Stat. 3618 (codified at 15 U.S.C. 8401 et seq.).

⁴ 15 U.S.C. 8402.

⁵ See Visa Core Rule 1.10.4.3, Cardholder and Transaction Information Disclosure Limitations. Exceptions apply for the provision of fraud control services or to support a loyalty program.

⁶ See "Visa Helps Protect Consumers from Deceptive Marketing," Visa Press Release (April 27, 2010); Visa Core Rule 5.9.15.1, Up-Selling Merchant Requirements.

November 13, 2014

Page 4

ROSCA to prohibit transfers of account information from one merchant to another in telemarketing transactions except to facilitate the processing of the original transaction in which the account information was originally acquired or to prevent fraud. Harmonizing the TSR with ROSCA would provide necessary industry clarity and benefit consumers by removing any doubt arising from potential inconsistencies. In addition, although each card network has taken its own respective steps to prohibit merchants from disclosing cardholder account information to third parties except to process the cardholder's initial sales transaction, curbing "data pass" and other questionable marketing schemes requires a multilayered response across the payments ecosystem and coordination among every business across the payments system to maintain consumer confidence. Addressing these practices through the TSR and enforcement at the federal level would further promote this objective and ensure that they do not migrate to other forms of payment to the detriment of consumers.

* * * *

Visa appreciates the opportunity to comment on this important matter. If you have any questions concerning these comments or if we can otherwise be of assistance, please do not hesitate to contact me at (202) 419-4109 or ktrantro@visa.com.

Sincerely,

Ky Tran-Trong
Vice President, Regulatory
Visa Inc.