sers@nictusa.com
06/03/2013 05:49 PM

To SERS@fec.gov, sersnotify,
cc
bcc
Subject New comment on REG 2013-01 submitted by Schrader, Russell

2 attachments

REG_2013_01_Schrader_Russell_06_03_2013_17_49_31_Visa Comments on FEC Technological Modernization ANPR.pdf

REG_2013_01_Schrader_Russell_06_03_2013_17_49_31_CommentText.txt

Please find attached the contents for the new comment submitted on Mon Jun 03 17:49:31 EDT 2013.
User uploaded 1 file(s) as attachment to the comment. Please find them attached to this email.
You will also find a Comment.txt file attached, which has the text comments entered by the user.
You may review the comment in FRAPS system. An approval action from FRAPS is required to send this comment event to the CMS. Thanks.

REG_2013_01_Schrader_Russell_06_03_2013_17_49_31_CommentText.txt

Attached are the comments of Visa Inc. on the Federal Election Commission's May 2, 2013 advance notice of proposed rulemaking on technological modernization.

Comments provided by :
Schrader, Russell

Russell W. Schrader
Senior Associate General Counsel
Global Enterprise Risk

June 3, 2013

By Electronic Delivery

Federal Election Commission
Attn.: Amy L. Rothstein
Assistant General Counsel
999 E Street, NW
Washington, DC 20463

Re: Technological Modernization, REG 2013-01

Ladies and Gentlemen:

This letter is submitted by Visa Inc. ("Visa") in response to the advance notice of proposed rulemaking and request for comment published by the Federal Election Commission ("FEC") on whether to begin a rulemaking to revise and modernize certain of the FEC's regulations to address, among other things, the increased use of electronic payments for political contributions ("ANPR").[1] Our comments are limited to the question posed in the ANPR about requiring political entities to retain payment card numbers. Visa appreciates the opportunity to offer its comments on this important issue.

Visa operates the Visa payment card network, and plays a pivotal role in advancing payment products and technologies worldwide. These payment cards, issued by participating banks, rather than Visa, are used by consumers, businesses and governments to complete payment transactions through a wide variety of payment card acceptance channels, including merchant point-of-sale terminals, the Internet and smartphones. Given Visa's role in consumer payments, Visa has a strong interest in ensuring that the use of payment cards and payment card information to complete transactions continues to be efficient and secure.

Legal Requirements Applicable to Payment Card Transactions

Visa strongly supports transparency in political contributions. Notwithstanding our support for the transparency of political contributions, we urge the FEC to be mindful of the fact that electronic payment transactions already are subject to a wide range of federal statutory and

[1] *See* Technological Modernization, 78 *Fed. Reg*. 25,635 (May 2, 2013).

Visa
P.O. Box 8999
San Francisco, CA 94128
U.S.A.

t. 650-432-1167
f 650-432-2145
rschrade@visa.com

regulatory requirements and interpretive guidance,[2] as well as private-sector network rules and requirements, like the Visa Rules.[3] Many of these requirements are designed to protect the security of payment transactions and prevent fraud, including fraud that results from identity theft. Before adding to or amending any existing regulations applicable to payment cards transactions, Visa strongly encourages the FEC to consider the impact that additional regulatory requirements could have on financial institutions and other entities that facilitate payment card transactions.

Standards Applicable to Payment Card Data Storage and Retention

The FEC has solicited comment on whether it would be appropriate to require, by regulation, that political entities receiving contributions through the use of payment cards (e.g., via credit card and debit card transactions) maintain records with the names and account numbers of the cardholders making such contributions. Prior to proposing any new record retention requirements for payment card transaction information, Visa strongly encourages the FEC to consider payment industry standards and best practices that are already in place to limit the storage and retention of payment card information.

Payment Card Industry Standards

The payment card industry, in partnership with other participants in payment card transactions, including merchants and payment processors, has developed a set of standards that apply broadly to all types of payment card transactions. These standards, known as the Payment Card Industry Data Security Standard ("PCI DSS"), are designed to safeguard both consumers and the payment system from fraud, particularly fraud resulting from data security breaches.[4] At the heart of the PCI DSS is the requirement that entities not store sensitive payment cardholder information, such as the information contained in the magnetic stripe of a card and the three-digit code printed on the back of payment cards, including Visa-branded cards, that is often used to complete transactions by phone or over the Internet. This is the type of information that criminals and hackers look to steal to create counterfeit cards and perpetrate fraud.

Where information, such as the payment card account number and the expiration date, is stored by entities that accept payment cards, it must be rendered unreadable in accordance with protocols established under the PCI DSS. This generally means that the account number must be

---

[2] Among the laws that apply to payment card transactions are the Electronic Fund Transfer Act, 15 U.S.C. §§ 1693 *et seq*.; the Truth in Lending Act, 15 U.S.C. §§ 1601 *et seq*.; and the Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6802 through 6809.

[3] For example, although the Visa Rules will apply to transactions involving Visa-branded cards, the rules of other payment card networks will apply if the transaction is not processed over the Visa network.

[4] The PCI DSS is a set of 12 detailed requirements designed around six principles fundamental to securing payment card data. For additional information about the PCI DSS, visit https://www.pcisecuritystandards.org/.

truncated, hashed or encrypted, so that unauthorized access to such payment card information will be of limited use to a criminal if a security breach occurs.

Any Regulatory Proposal Should Take into Account Industry Standards

It is important for the FEC to recognize that political committees and other entities are subject to the PCI DSS, typically by contract, when they accept payment cards as a form of payment.[5] Visa urges the FEC to avoid any regulatory approach that would result in a mandate that is inconsistent with the industry best practices established by the PCI DSS. Specifically, the FEC should not propose any regulatory requirements that would be prohibited by the PCI DSS.

* * * *

Visa appreciates the opportunity to comment on the ANPR. If you have any questions, or if I can otherwise be of assistance, please do not hesitate to contact me at (650) 432-1167.

Sincerely,

Russell W. Schrader
Senior Associate General Counsel and
Chief Privacy Officer
Visa Inc.

dc-719169

[5] In addition, we note that at least one state, Nevada, has enacted a statute that mandates compliance with the PCI DSS in connection with payment card acceptance and the sale of goods or services. *See* Nev. Rev. Stat. § 603A.215.