

**Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554**

In the Matter of)	
)	
Petition for Exemption of the American Bankers Association)	CG Docket No. 02-278
)	
Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991)	

**COMMENTS OF MASTERCARD INCORPORATED IN SUPPORT OF THE
PETITION FOR EXEMPTION OF THE AMERICAN BANKERS ASSOCIATION**

MasterCard Incorporated (“MasterCard”)¹ hereby submits these comments in support of the petition for exemption of the American Bankers Association (“Petitioner”) that was filed with the Commission on October 14, 2014 (the “Petition”). The Petition requests that the Commission exempt the following types of time-sensitive information calls from the restrictions in the Telephone Consumer Protection Act (“TCPA”), 47 U.S.C. § 227, as implemented by the Commission at 47 C.F.R. § 64.1200: automated calls and text messages sent to wireless telephone numbers related to:

- Transactions and events that suggest a risk of fraud or identity theft;
- Possible breaches of the security of customers’ personal information;
- Steps consumers can take to prevent or remedy harm caused by data security breaches; or

¹ MasterCard is a technology company in the global payments industry. We operate the world’s fastest payments processing network, connecting consumers, financial institutions, merchants, governments and businesses in more than 210 countries and territories. MasterCard’s products and solutions make everyday commerce activities—such as shopping, traveling, running a business and managing finances—easier, more secure and more efficient for everyone.

- Money transfer notifications.

MasterCard supports the petition and respectfully urges the Commission to grant the requested exemption. Doing so will facilitate prompt and efficient communication of time-sensitive information that can both limit the occurrence of fraud and identity theft and mitigate the impact when it does occur.

Background on MasterCard.

MasterCard does not issue payment cards of any type, nor does it contract with merchants for acceptance of those cards. In the MasterCard payment system, those functions are performed in the United States by numerous banks. MasterCard refers to the banks that issue payment cards bearing the MasterCard brands as “issuers.” MasterCard refers to the banks that enter into contracts with merchants to accept MasterCard-branded payment cards as “acquirers.” MasterCard owns the MasterCard family of brands and in the United States licenses banks to use those brands in conducting payment transactions. MasterCard also provides the networks through which its customer banks can interact to complete payment transactions, and sets certain rules regarding those interactions.

When a cardholder presents a MasterCard-branded payment card to a merchant to purchase goods or services, the merchant sends an authorization request to its acquirer, the acquirer routes the request to MasterCard, and MasterCard routes the request to the issuer. The issuer either approves or declines the authorization and routes its decision back to the merchant through the same channels. MasterCard’s role in the transaction is to facilitate the payment instructions between the acquirer and the issuer.

As part of facilitating the transaction, MasterCard provides services to acquirers and issuers to help detect potentially fraudulent transactions. In addition, issuers have developed their own programs to detect and block potentially fraudulent transactions.

MasterCard's Interest. MasterCard has a strong interest in the security of payment card information and, as such, fully supports the limited exemption requested by the Petition because, in part, the safe operation of the payment network depends on the avoidance of fraudulent transactions being processed. Fraudulent transactions can result in a negative impact on cardholders and merchants and may lead to consumers' being less willing to undertake and merchants willing to accept payment card transactions that are processed over the MasterCard network. In addition, if there is an increase in fraudulent charges, the processing of disputes and reversals of those charges imposes additional demands on our network.

MasterCard's rules require issuers and acquirers to follow data security standards that have been adopted by the PCI Security Standards Council. Acquirers are required to cause merchants to follow the PCI Data Security Standards. These rules are designed to ensure the proper protection of transaction information to prevent data breaches and the fraud that can result. MasterCard's rules also contain provisions about liability of issuers and acquirers in the event of fraudulent transactions, as well as in the event of data security incidents and unauthorized transactions that may result from those incidents. As a result, MasterCard has a strong interest in efforts that may minimize the occurrence of fraud and identity theft.

Security Breaches. Recent years have seen a number of data security breaches affecting cardholders, including breaches involving national merchants that have attracted

extensive media attention as well as smaller breaches that receive little or no publicity. Regardless of the size of the breach, these incidents can have a direct impact on cardholders in the following ways:

- Fraudsters may use stolen account information to initiate unauthorized charges to cardholder's accounts;
- Fraudsters may use stolen contact information to engage in "phishing" and similar attempts to get information from cardholders; or
- Issuers may need to re-issue payment cards, requiring cardholders to change recurring payment authorizations.

Generally, existing law protects cardholders from incurring liability for unauthorized charges; however, cardholders still need to monitor their accounts for potentially unauthorized charges and may need to notify their issuers of these unauthorized charges.

Importance of Prompt and Effective Consumer Notice. Notifying cardholders of potentially fraudulent transactions and data breach incidents, and the potential impact on them, is extremely important.

For potentially fraudulent transactions, MasterCard's and issuers' systems are very sophisticated predictors of fraud. There are situations where a transaction that is potentially fraudulent is detected, and it requires contacting the cardholder to determine whether the transaction should be allowed. If an issuer can send a real-time (or near real-time) communication regarding a suspicion of fraud to the affected consumer, then the cardholder can either confirm that the transaction was fraudulent—in which case additional steps can be taken to stop that transaction as well as future fraudulent transactions—or the cardholder can confirm that the transaction was legitimate—in

which case the transaction can be authorized. Speed of communication is essential in these circumstances. Otherwise, proactive measures to detect fraud may be delayed, or a wholly legitimate transaction may not occur.

Requiring that a notice be sent by mail would impose unnecessary and costly delays in getting this information to consumers. In addition to the time that it takes to print the mailing, it often takes several days for mail to be delivered, and cardholders may not open such a mailing immediately (if at all). E-mail is often not a viable alternative for many cardholders, since issuers may not have e-mail addresses for a large percentage of their cardholders.

Text messages and automated calls, however, are more likely to reach cardholders quickly. And messages or calls directed at wireless telephone numbers are the most likely to reach cardholders in a timely manner. First, many consumers only have wireless telephone numbers. Second, consumers may not be at their home or in their offices when conducting a transaction (indeed, they may be at a merchant location), but they are likely to have their wireless devices with them. As a result, consumers can receive the message or call promptly, and then take action.

In the case of a data breach event, individually dialed phone calls may also not be practicable because the number of consumers affected can number in the hundreds of thousands or even millions. And yet, even in situations where a data breach incident receives substantial media attention, the ability to send prompt, targeted messages to consumers is important. Consumers may not understand, based on media reports, whether they are included in a group put at risk by an incident, and they may not understand what actions they can take to mitigate any exposure. Targeted messages can

provide that type of information quickly and directly to the consumers who can then act upon it.

The types of messages that Petitioner has requested be exempted from the TCPA requirements would facilitate prompt notice to consumers without unnecessary risk to cardholder privacy. Consumers would be able to take steps to minimize fraud and identity theft. The limited exemption requested would allow these communications to occur without fear of liability for unintended violations of the TCPA.

Three Benefits of Prompt Notice. There are at least three significant benefits to cardholders and payment card networks, including MasterCard, that can follow from allowing prompt notice in the form requested by the Petition.

First, prompt notice can prevent fraudulent transactions from occurring. A near real-time notice sent to a consumer can allow that consumer to confirm that a transaction is fraudulent—allowing the transaction to be blocked before it occurs. And, once a single fraudulent transaction is detected, the cardholder and the issuer can discuss whether additional steps—such as reissuance of the card—are warranted.

Second, prompt notice can allow legitimate transactions to occur. If a transaction is declined because of suspected fraud, then the consumer may not be able to complete the transaction or may need to use a less favored payment method. A near real-time message, however, can prompt the cardholder to contact his or her issuer to confirm that a transaction is legitimate, enabling the transaction to be completed as originally requested by the cardholder.

Third, prompt notice can allow issuers to take appropriate remedial actions for fraudulent transactions that do occur. If a cardholder confirms that a transaction was

fraudulent, for example, the issuer can initiate the process of reversing that transaction. The issuer can also discuss other transactions with the cardholder to see if they are also fraudulent, and can suggest steps—such as card reissuance—to prevent additional fraud.

Protecting Consumers and Their Privacy. MasterCard also agrees with Petitioner that appropriate conditions should be built into the exemption to protect consumers and their privacy. First, messages should be sent only in a manner that imposes no costs on the consumer, and that does not count against a consumer's plan minutes or texts. In addition, as proposed by Petitioner, the exemption could be conditioned on:

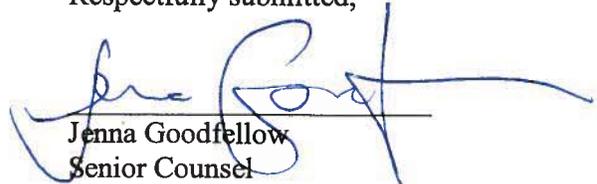
- Sending the messages specifically to consumers who are impacted by the incident, or to whom a specific alert should be directed.
- Identifying the name of the financial institution sending the message, and including contact information.
- Containing only content related to the potentially fraudulent transaction or the security compromise, and not containing any marketing or advertising.
- Being short and concise.
- Limiting the number of messages to what is required to complete the purpose.

Conclusion. Technological developments have provided many benefits to consumers, including new ways to use payment cards that are processed over payment card networks. At the same time, technological developments also have created new risks, such as more prevalent fraudulent transactions and data breaches. It is important to allow technologies to be used to mitigate these risks. MasterCard and issuers have

developed models to detect fraud and protect consumers from fraudulent activity. These efforts can be significantly enhanced by facilitating prompt and effective consumer communications. Consumers have adapted to using their mobile devices in ways that were not anticipated when the TCPA and the Commission's existing rules were enacted. Under these circumstances, the limited exemption requested by the Petition is appropriate to allow financial institutions to provide prompt and effective notice of potential fraud and security incidents to their customers.

MasterCard therefore supports the Petition and urges the Commission to act promptly to grant the requested exemption.

Respectfully submitted,

A handwritten signature in blue ink, appearing to read 'Jenna Goodfellow', is written over a horizontal line.

Jenna Goodfellow
Senior Counsel
U.S. Regulatory and Public Policy
MasterCard Incorporated
2000 Purchase Street
Purchase, New York 10577-2509

Dated: December 8, 2014