RICHARD BLUMENTHAL
CONNECTICUT

COMMITTEES:

AGING

ARMED SERVICES

COMMERCE, SCIENCE, AND TRANSPORTATION

JUDICIARY

VETERANS' AFFAIRS, RANKING MEMBER

United States Senate

WASHINGTON, DC 20510

706 HART SENATE OFFICE BUILDING
WASHINGTON, DC 20510
(202) 224-2823
FAX: (202) 224-9673

90 STATE HOUSE SQUARE, TENTH FLOOR
HARTFORD, CT 06103
(860) 258-6940
FAX: (860) 258-6958

915 LAFAYETTE BOULEVARD, ROOM 230
BRIDGEPORT, CT 06604
(203) 330-0598
FAX: (203) 330-0608

http://blumenthal.senate.gov

August 3, 2015

Mr. Brian Mooney
Interim CEO
Merchant Customer Exchange
160 Gould Street, Suite 205
Needham, Massachusetts 02494

Dear Mr. Mooney:

As a member of the Senate Commerce, Science, and Transportation Committee, I am closely following technology developments that enhance the security and privacy of personal information and data. One such emerging technology discussed at a recent hearing is the use of tokenization in mobile payments. At this hearing, the representative from the National Retail Federation disputed that retailers were unreasonably blocking this technology, suggesting instead that the technology is "unproven" or "extraordinarily expensive." I am concerned by the mischaracterization of this technology and write to better understand this conclusion.

As you know, tokenization allows mobile payment systems to create and transmit a unique numerical code for each transaction, reducing the circulation of sensitive financial information and the risk of fraud. The Visa Token Service, currently used for Visa Checkout and digital wallets including Android Pay, Apple Pay, and Samsung Pay, uses a secure payment tokenization for consumers to purchase goods and services quickly and easily while safeguarding their name, credit card number, and security code. Mobile payment systems utilizing tokenization are a leap forward in privacy and security and a valuable new option for consumers. It would seem a clear benefit to consumers for this technology to be widely available through terminals that are already installed, so as to hasten its adoption and decrease the risk of theft and fraud.

For this reason, I am concerned by reports that some merchants are banding together to deny consumers the option of conducting transactions with this new technology. Apple Pay launched in the fall of 2014 with a large number of participating merchants and financial institutions. Among the participating merchants, only a few seem to also be members of the Merchant Customer Exchange (MCX) which is working on a competing payment system, CurrentC. A few days after the launch of Apple Pay, it was reported that some MCX members disabled their near field communication (NFC) terminals that had been in use for years to accept contactless credit card transactions, apparently in order to block consumers from using digital wallets that depend on the same NFC-enabled terminals. As a direct result, consumers are also being blocked from using more secure payment methods and required to provide potentially sensitive personal information to these merchants.

At the same time that consumers were denied innovative payment options providing greater privacy and security, MCX disclosed that a significant security breach occurred within the technology under development[1]. The theft of financial records and personal information undermines consumer confidence and imposes unnecessary costs on consumers, businesses, and the economy. Consumers should not be denied payment options that protect their personal privacy and financial data, and businesses should not act in concert to stifle competition.

Payment systems using tokenization have the potential to revolutionize commerce by reducing fraud, increasing privacy and security, and saving money for both consumers and businesses. To realize the many benefits of this new technology, all tokenization systems must be given a fair opportunity to compete.

In order to better understand the potential benefits of tokenization and your organization's decision and/or the individual decision of some of your members to disable the NFC readers in retail locations, please provide answers to the following questions:

- Are MCX members prohibited from using competing mobile wallet payment platforms such as Apple Pay? If so, has MCX actively enforced any such prohibition?
- Explain how consumers benefit by the prohibition on MCX members from enabling their POS terminals to be used by competing mobile wallet payment platforms.
- Are there circumstances under which MCX members will be allowed to accept payment through competing mobile wallet payment platforms?
- Provide a copy of the contract MCX members sign to enter the network.
- What transaction data does MCX collect in connection with a consumer purchases?
- With whom does MCX share any personal and transaction data collected at the point of sale?
- How is an individual's financial account protected through the use of the MCX platform?
- Provide a full and complete briefing on the data breach at MCX exposing consumer emails including how the breach was detected, how long the breach occurred before being discovered, how many emails were stolen, what other information was stolen, what steps MCX has taken to safeguard against further loss, what steps MCX members are taking to protect against data breaches, and if further data breaches have been detected.

I ask that you provide your answers by August 30, 2015. Thank you for your attention to this issue.

Sincerely,

Richard Blumenthal
United States Senate

[1] http://www.mcx.com/blog/1028-email-incident-report/