December 15, 2014

Thomas J. Curry
Comptroller of the Currency
400 7th Street, SW
Washington, D.C. 20219

Dear Comptroller Curry,

We wanted to bring to your attention statements made by OCC Senior Critical Infrastructure Officer Valerie Abend in testimony before the Senate Banking Committee on December 10th. Unfortunately, Ms. Abend appears to be uninformed about the way the payment card system operates to push liability onto merchants when there are data breaches – wherever those breaches happen. It is important for policymakers to have all the facts regarding data breaches so they can make informed decisions about economic incentives and how policy should interact with currently existing incentives. If they get inaccurate information from regulators, it could lead to policy solutions that do not do what policymakers expect and do not address the problems in this area adequately. In the future, we hope that OCC officials research these issues and portray them accurately to improve the quality of congressional deliberations.

I would like to take this opportunity to dispel a few misconceptions, echoed in Ms. Abend's testimony and your own comments to the Community Bankers Symposium this fall, which seem to have arisen regarding recent cyber-attacks and the response by retailers and financial institutions. Contrary to the testimony:

- **Retailers share the costs incurred by card fraud.**

A 2013 study by the Federal Reserve looked at fraud instances in debit cards and found that this was the case. In fact, costs were shown to be borne almost equally among retailers and card-issuing institutions. These vary by transaction: for more secure PIN debit transactions the card issuer, naturally, absorbed a greater share of the fraud; for less secure signature debit transactions the merchants absorbed nearly half of all fraud losses; and for card-not-present debit transactions (transactions made online, over the telephone or by catalogue) merchants bear a greater percentage of fraud losses than card issuers do. And, merchants pay the cost of card fraud in advance, through swipe fees, before fraud is ever incurred. In fact, even the Federal Reserve's debit card regulations are geared to provide that the average issuer has one hundred percent of its debit fraud losses covered by swipe fees. Not to mention, even after absorbing substantial fraud losses, merchants are subject to massive fines by Visa and MasterCard networks and hundreds of millions of dollars in restitution through private litigation for cybersecurity breaches.

In fact, merchants who suffer data breaches, according to card network rules, must pay for the additional fraud made with cards that have been compromised. There is no such reciprocal responsibility for financial institutions. When they have breaches, they do not cover the fraud losses absorbed by merchants.

Ms. Abend's call to "even the playing field" then is upside down. Merchants pay more than one hundred percent of the banks' fraud losses – some prepaid through swipe fees and some paid after the fact. If the playing field needs to be leveled, it means that institutions regulated by the OCC need to give up some of those funds and cover more of the fraud losses incurred so that merchants are not paying for more than one hundred percent of the card fraud.

- **Retailers pay the costs of issuing new cards to consumers after a data breach.**

Merchants do, in fact, reimburse card issuers for both card reissuance following a breach based on many factors, including: the number of cards requiring reissuance, and the age of the card and when it was due for reissuance regardless of a breach. These schedules are contractually agreed upon by Visa and MasterCard and the financial institutions with which they work. Merchants do not have a say in these reimbursement requirements. For example, MasterCard requires merchants to reimburse card issuers on the following schedule for card reissuance:

Reimbursement Rate Per Tier

Tier	Issuer—Gross Dollar Volume	Mag Stripe	Chip[2]	*PayPass*	Combo[3]
1	0–200 MM	USD 2.69	USD 3.66	USD 3.44	USD 4.04
2	201 MM–1 B	USD 2.31	USD 3.29	USD 3.06	USD 3.66
3	> 1B	USD 2.00	USD 2.98	USD 2.75	USD 3.35

A fixed deductible of 40 percent is subtracted from the gross eligible reimbursement amount to reflect anticipated card expirations and accounts published in previous MasterCard Alerts.

This chart clearly shows that institutions with assets of under $200 million are eligible to receive a higher reimbursement rate than their larger competitors. Additionally, if there is fraud associated with the card, card issuers are again eligible for a separate fraud adjustment reimbursement. Visa's rules operate in a similar way.

These costs are also covered by merchants up front through payment of swipe fees on every card transaction. The Federal Reserve's regulations on debit fees, for example, specifically provide for a one cent fraud prevention fee on every debit transaction for institutions that meet fraud prevention standards. The regulations include the cost of re-issuing cards in that fee. Credit fees, of course, are much higher than debit fees and cover these types of costs many times over.

Ms. Abend's testimony then that card-reissuing costs put larger burdens on small institutions ignores the fact that these costs are prepaid to financial institutions by merchants, ignores the graduated scale of reimbursement that merchants provide when they have data breaches – and, in fact, ignores that merchants pay for the re-issuance of cards at all.

- **Financial institutions have more data breaches than other industries.**

Ms. Abend chose to focus on merchant data breaches in her testimony even though more breaches occur at financial institutions. This is true even though there are 1,000 times as many merchants in the United States as there are banks and credit unions. When the 2014 Verizon Data Breach Investigations Report analyzed 1,367 data-loss incidents last year, they found that 465 (roughly 34 percent) took place at financial institutions, while less than 150 (less than 11 percent) affected retailers. Furthermore, the recent breach at J.P. Morgan Chase & Co. – one of the largest financial institutions in the world – is reported to have compromised the information of some 76 million households and seven million businesses. And, as the USA Today reported on its front page October 20th, "Federal officials warned companies Monday that hackers have stolen more than 500 million financial records over the past 12 months, essentially breaking into banks without ever entering a building." It is important to realize that both retailers and financial institutions have been affected by cyber-attacks and both likely will be again.

- **Merchants make large investments in data security.**

Just like data breaches are a shared threat, protecting against them is a shared responsibility. Merchants spend more than $6 billion every year on data security. And retailers already employ a number of methods to protect against card fraud, including:

- PIN prompting at the point-of-sale for debit cards
- Card Verification Value (CVV) prompting for Internet purchases
- Address/ZIP code verification
- Automated transaction scoring
- Data encryption
- Data tokenization
- Internet Protocol (IP) address/geolocation authentication

Merchants pay financial institutions extra for some of these services. And, in addition to the safeguards listed above, retailers are proactively leading the way in advancing technology that would significantly increase protection for consumers: Chip-and-PIN payment cards.

The volume of cyber-attacks in the United States is particularly intense because of the antiquated and woefully inadequate magnetic stripe technology still in place today. As issuing banks in nearly every other G-20 nation have migrated away from this 1960s-era technology to a substantially more secure technology, known as Chip-and-PIN, cybercrime and fraud have migrated to the United States. Retailers are on track to have completed an enormous investment in order to be able to accept these cards. Yet, there is still little promise that card issuers will issue such cards. In fact, financial institutions trail merchants on these technology updates in the United States and around the globe. Outside of the U.S., seventy percent of merchants have upgraded to Chip-and-PIN devices at the point-of-sale, but only forty percent of the cards have been upgraded. That is similar to the situation in the United States in which nearly twenty

percent of merchants have upgraded but less than one percent of the cards issued have the new technology.

Unfortunately, card issuers in the United States intend to begin issuing chip cards without requiring PINs, a feature that is proven to reduce fraud by 700 percent on debit cards alone. This is an inexcusable lapse which threatens to make billions of dollars in merchant upgrades ineffective. It's hard to ignore the benefits of PINs for enhanced security when financial institutions themselves require them for ATM withdrawals. Card issuers seem to value their security over that of merchants and consumers. Signatures do not do anything to protect against fraud and should be eliminated as a way to show the authenticity of card transactions. We need to use PINs or other methods that provide enhanced security to protect against fraud.

* * *

It would have enhanced the Senate Banking Committee's understanding of the facts and the issues relating to data security if Ms. Abend's testimony had reflected this information. In the future, we hope that the OCC will check the facts and engage in dialogue with groups it might mistakenly be maligning – in this case our members – before submitting testimony on these topics. Toward that end, we would like to meet with you to discuss these issues so that you have the benefit of our perspectives. Please contact Doug Kantor at (202) 429-3775 or dkantor@steptoe.com to let us know when such a meeting might be possible.

Sincerely,

Food Marketing Institute
National Association of Convenience Stores
National Grocers Association
National Restaurant Association
National Retail Federation
Retail Industry Leaders Association

cc: Members of the Senate Banking Committee