December 29, 2014

Mr. Camden R. Fine
President and CEO
Independent Community Bankers of America (ICBA)
1615 L Street, NW
Suite 900
Washington, D.C. 20036

Dear Mr. Fine,

Your organization recently issued a press release entitled "Community Banks Reissue Nearly 7.5 Million Payment Cards Following Home Depot Data Breach," which detailed the results of a survey of community banks in the wake of the Home Depot cyber-attack earlier this year. The release also outlined a number of policy proposals.

Regrettably your release – including the quotation from ICBA's Chairman John Buhrmaster – contained a number of inaccuracies and misrepresentations. We write to you today in order to address these misleading points and to address the policy changes for which your organization is advocating.

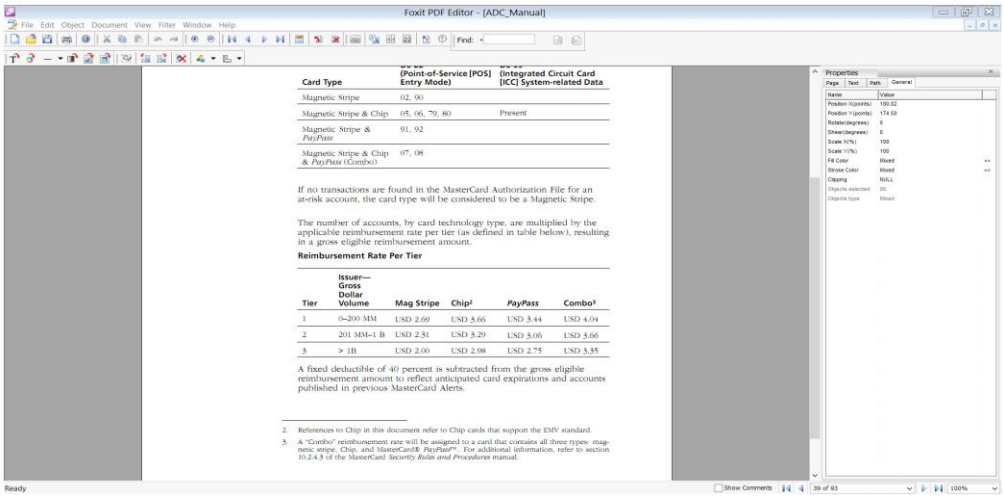
For the sake of our customers and all American consumers, it is crucial that organizations like ours work together in order to make electronic payments more secure. By clearing up misinformation and fostering open dialogue, it is our hope to achieve this common and critical goal.

At the outset, it is important to acknowledge that the cyber-criminals who perpetrate these attacks do not exclusively target retailers. Financial institutions – including your member community banks – face the same or greater levels of risk. The 2014 Verizon Data Breach Investigations Report, which analyzed 1,367 incidents of data loss last year, found that 465 (about 34 percent) of such incidents affected financial institutions. However, fewer than 150 incidents (less than 11 percent) took place at retail stores. One of the world's largest banks, J.P. Morgan Chase & Co., was targeted this summer in a massive breach that compromised some 83 million accounts. A *USA Today* report in October cited Federal Bureau of Investigation (FBI) officials stressing the vulnerability of banks by observing that "hackers have stolen more than 500 million financial records over the past 12 months." ICBA cannot simply dismiss data breaches as a retail problem and refuse to recognize the risk to financial institutions – to do so would be a disservice to your members.

Changes in policy – and in the way we in the electronic payment sphere do business – will be necessary to combat these ever-changing and ever-growing cyber-threats. Unfortunately, the principles that ICBA outlined in your recent release are based in part on misinformation and at best incomplete. We would like to take this opportunity to respond to the principles below.

- **Retailers bear more of the costs of breaches than banks.** Retailers pay more than one hundred percent of the costs associated with breaches at their stores. For ICBA Chairman

Buhrmaster to state that "[c]ommunities and customers should not suffer for the faults of retailers" is to insinuate that merchants are shirking their responsibility and this is simply inaccurate. A 2013 study of debit card fraud conducted by the Federal Reserve found that retailers share the costs of all card fraud. Those costs were shown to fall mostly equally among retailers and the financial institutions that issued the compromised cards. The exact breakdown varies by the type of transaction: for more secure PIN debit transactions the card issuer 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 (payments made online, over the telephone or by catalogue) merchants assumed a greater percentage of fraud losses than card issuers. Merchants also pay the cost of card fraud in advance through swipe fees before any fraud even occurs. The Federal Reserve's debit card regulations are specifically designed so that these swipe fees provide the average issuer with one hundred percent coverage for all debit card fraud losses – including those caused by bank breaches. Those regulations also make retailers pay the costs of re-issuing cards. Retailers are further subject to fines by Visa and MasterCard, along with hundreds of millions of dollars in restitution through litigation. Specific to the concerns addressed in ICBA's release, merchants contribute to the costs of reissuing cards not only through swipe fees but through contractual agreements between Visa and MasterCard and your member institutions. Retailers do not have a say in these reimbursement requirements. For example, MasterCard reimburses card issuers on the following schedule for card reissuance:


Foxit PDF Editor - [ADC_Manual]

Card Type	(Point-of-Service [POS] Entry Mode)	(Integrated Circuit Card [ICC] System-related Data
Magnetic Stripe	02, 90	
Magnetic Stripe & Chip	05, 06, 79, 80	Present
Magnetic Stripe & *PayPass*	91, 92	
Magnetic Stripe & Chip & *PayPass* (Combo)	07, 08	

If no transactions are found in the MasterCard Authorization File for an at-risk account, the card type will be considered to be a Magnetic Stripe.

The number of accounts, by card technology type, are multiplied by the applicable reimbursement rate per tier (as defined in table below), resulting in a gross eligible reimbursement amount.

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.

2. References to Chip in this document refer to Chip cards that support the EMV standard.
3. A "Combo" reimbursement rate will be assigned to a card that contains all three types: magnetic stripe, Chip, and MasterCard® *PayPass*™. For additional information, refer to section 10.2.4.3 of the MasterCard *Security Rules and Procedures* manual.

This chart shows that a financial institution with assets of under $200 million is eligible to receive a higher reimbursement rate than its larger competitors. Additionally, if there is fraud associated with the card, card issuers are again eligible for a separate fraud adjustment reimbursement. More details can be found in the following sections of MasterCard's operating rules: 6.4.1 ADC Operational Reimbursement Factors, MasterCard Account Data Compromise User Guide, July 22, 2012. Visa has similar agreements in place as well.

- **The Gramm-Leach-Bliley Act is not a model for data security.** We certainly support federal breach notification legislation to ensure consistent and clear communication with the

customers who patronize our stores and your banks. The current system of relying on varying state laws is unsustainable. Our shared customers would be better served by a single federal framework that recognizes operational realities and is proportional to risk of harm. However, the Gramm-Leach-Bliley Act standards, which ICBA advocates expanding to merchants, is not the ideal template for future legislation. For example, under GLBA, banks are not required to inform their customers about potential breaches. In fact, banks have significant discretion over what customers are actually told under the law – and whether they are told anything at all.

- **We need increased sharing of information between law enforcement and the business community, as well as between retailers and financial institutions.** This is an area where good-faith involvement of all parties is important. Retailers promote cooperation and the sharing of cyber threat information within the retail industry through the Retail Cyber Intelligence Sharing Center (R-CISC), but engage consistently with stakeholders outside our own sector as well. Also, the Merchant Financial Cyber Partnership is made up of some 250 senior executives at retailers and financial institutions – including ICBA – who work together to facilitate greater collaboration between our industries against cybercrime. We appreciate working with the ICBA as part of the partnership, but find accusations like those in your recent press release to be extremely counterproductive to our joint efforts.

- **Ignoring PIN technology leaves us all more vulnerable.** While ICBA supports the movement to embedded-chip technology for credit and debit cards, the organization appears to only do so grudgingly, questioning its efficacy against data breaches. Furthermore, ICBA only references general "chip technology" and not the more secure type – "chip-and-PIN" – for which we are advocating. "Chip-and-PIN" has already shown success throughout the world and could reduce fraud losses in the U.S. by as much as 40 percent, according to the Federal Reserve Bank of Kansas City. The added security provided when each customer is given a unique personal identification number or PIN has already been shown to make debit card transactions 700 percent safer. Alternatives such as "chip-and-signature" do not provide this level of security. Furthermore, PINs would also make "card-not-present" transactions safer by adding another layer of authentication. While no technology will be able to prevent all cyber-attacks, anytime, anywhere, it is worth noting that stronger security might have resulted in fewer cards being compromised in recent breaches and therefore fewer reissuances by banks. The sooner this migration is begun in earnest, the better. Indeed, banks reissuing less-secure magnetic-stripe cards to their customers only contributes to the cycle of breaches and data loss. These types of cards, using 1960s-era technology, have been identified in a recent report by Trend Micro as likely being behind the United States' ranking as the worst country in the world for point-of-sale malware infections. Retailers are already well underway in their efforts to install "chip-and-PIN"-capable sales terminals in stores across the country. Even the federal government is making the switch to "chip-and-PIN" starting next year. ICBA needs to support PIN technology and not just the chip cards which, by themselves, will not be very effective.

We appreciate the opportunity to correct this misinformation. Protecting our customers' personal information is an important goal, which we cannot allow to be sidetracked by

inaccuracies. We hope that, in the future, the ICBA will stick to the facts as we work and advocate together to help secure the payments system.

Sincerely,

Sandra L. Kennedy
President
Retail Industry Leaders Association

Henry Armour
President and CEO
National Association of Convenience Stores

Matthew R. Shay
President and CEO
National Retail Federation

Leslie G. Sarasin, Esq., CAE
President and CEO
Food Marketing Institute

Peter J. Larkin
President and CEO
National Grocers Association

Dawn Sweeney
President and CEO
National Restaurant Association

Mark Horwedel
CEO
Merchant Advisory Group