

November 7, 2016

Submitted Electronically - www.regulations.gov

Mr. David Lincicum and Ms. Katherine McCarron
Division of Privacy and Identity Protection, Bureau of Consumer Protection
Federal Trade Commission
Office of the Secretary
600 Pennsylvania Ave. NW
Suite CC-5610 (Annex B)
Washington, DC 20580

RE: Safeguards Rule, 16 CFR 314, Matter No. P145407

Mr. Lincicum and Ms. McCarron:

I am writing on behalf of the National Association of Convenience Stores (“NACS”) and we appreciate this opportunity to comment on the Federal Trade Commission’s (“FTC”) Standards for Safeguarding Customer Information (“Safeguards Rule”). NACS is an international trade association representing the convenience store industry with more than 2,200 retail and 1,800 supplier companies as members, the majority of whom are based in the United States.

The convenience store industry as a whole operates approximately 154,000 stores across the United States. In 2015, the industry employed more than two and a half million workers and generated \$574.8 billion in total sales, representing approximately 3.2 percent of the U.S. GDP. In light of the number of fuel and other transactions in which our industry engages, we handle approximately one of every 30 dollars spent in the United States. Our retailers serve about 160 million people per day – around half of the U.S. population – and our industry processes over 73 billion payment transactions per year. Nevertheless, the convenience store industry is truly an industry of small businesses. Approximately 63 percent of convenience store owners operate a single store, and approximately 75 percent of the industry is composed of companies that operate ten stores or less.

As noted in your September 7, 2016 request for public comment, the FTC’s Safeguards Rule currently applies to “financial institutions,” defined as institutions significantly engaged in financial activities.¹ To date, the FTC has refrained from extending the definition of “financial institution” to encompass entities engaged in activities merely “incidental” or “complementary” to financial activities—an approach upon which the FTC seeks comment.²

NACS urges the FTC not to expand its definition of “financial institution” or attendant Safeguards Rule requirements beyond businesses that conduct traditional financial activities (e.g., lending, exchanging, investing for others, guaranteeing, providing financial or advisory

¹ 81 Fed. Reg. 61633 (Sept. 7, 2016).

² *Id.*

services, underwriting, etc.).³ While traditional financial institutions are uniquely equipped and appropriately positioned to fulfil the Safeguards Rule’s obligations, incidental participants in financial transactions such as our members are not. For instance, convenience stores, unlike financial institutions, do not store customer information, nor do they have continuing information-based relationships with consumers that would justify development and maintenance of a comprehensive security program.⁴ And, our members’ stores do not handle some of the most sensitive identifying information of consumers – such as social security numbers, driver’s license numbers and the like – that lead to identity theft. Financial institutions, by contrast, do handle that type of data.

Notwithstanding the foregoing, NACS members are dedicated to preserving their customers’ trust and protecting their security. Consequently, they invest heavily in reducing fraud in the payment card system.⁵ The most effective security measure available today to protect against fraud in payment card transactions is the use of personal identification numbers (“PINs”). In fact, the Federal Reserve Board has found that PIN is *six times* more secure than signature authentication of card transactions.⁶ Financial institutions, however, have consistently pursued (and indeed, aggressively pushed for) a PIN-less path in the United States.

For example, the recent shift to EMV chip technology imposed by financial institutions on U.S. retailers could and should have included chip *and* PIN capability so that merchants had the option of protecting transactions that might be subject to fraud. Instead, however, this technology was introduced in the U.S.—unlike other parts of the world—with a chip-only approach. This move puts U.S. consumers and businesses at unnecessary risk given PIN’s proven record at reducing fraud (with or without a chip) and the success of chip and PIN in other countries. Indeed, Visa advertises the benefits of chip and PIN on its own website, noting that in the United Kingdom, fraud related to lost and stolen payment cards has decreased by more than half since chip and PIN was adopted there in 2014.⁷

Furthermore, banks, unlike merchants, have the option of requiring PINs at their ATMs—and every bank of which we are aware does so. Clearly, the financial institutions recognize and take

³ See 12 U.S.C. § 1842(k)(4).

⁴ See 81 Fed. Reg. 61633 (noting Safeguards Rule does not apply to all consumer information, but rather to information of customers, which are consumers that have a continuing relationship with a financial institution; also describing the general obligation for financial institutions to develop, implement and maintain a comprehensive information security program to safeguard customer information they “access, collect, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle”).

⁵ Further, merchants pay for fraud losses at a much higher rate than financial institutions, thereby bolstering our members’ incentives to prevent fraudulent transactions. See LexisNexis and Javelin Strategy Research, annual report, *True Cost of Fraud* (2009) (retailers suffered fraud losses 10 times higher than financial institutions); Consumer reports, *House of Cards: Why your Accounts are Vulnerable to Thieves* (June 2011) (retailer fraud losses of tens of billions of dollars a year dwarfs card issuer losses).

⁶ Federal Reserve Board, Debit Card Interchange Fees and Routing, 77 Fed. Reg. 46261 (Aug. 3, 2010).

⁷ *The Benefits of Chip and PIN for Merchants*, available at <http://www.visa.ca/chip/merchants/benefitsofchippin/index.jsp> (last visited Sept. 21, 2015).

advantage of the security benefits of PIN. NACS members and other merchants, on the other hand, are prohibited under the card companies' operating rules from requiring customers to enter a PIN number when accepting a payment card. This structure simply does not make sense from the perspective of maximizing consumer protection or card transaction security.

The FTC has requested comment on what modifications should be made to the Safeguards Rule to increase its benefits to consumers. In light of the above, NACS urges the FTC to, at a minimum, require financial institutions to make sure that their products are enabled with secure technology (today, that means enabling PINs on all payment cards), and to adopt/promote strong security measures. As security measures evolve and improve, financial institutions should be required to keep pace in order to *effectively* protect customers and their information.

Again, NACS appreciates this opportunity to comment on the FTC's Safeguards Rule and we thank you for your consideration.

Sincerely,

/



l

Lyle Beckwith
Senior Vice President, Government Relations
National Association of Convenience Stores