ELECTRONIC TRANSACTIONS ASSOCIATION

1101 16th Street NW
Suite 402
Washington, DC 20036

www.electran.org
T 800.695.5509
T 202.828.2635
F 202.828.2639

Dear Attorney General:

As you are probably aware, the payments industry has initiated the most significant upgrade to our nation's credit and debit cards in decades, in order to increase security for consumers, retailers, and the overall payments system.

The transition to EMV or "chip" cards is a major priority because EMV addresses the most common form of in-store fraud — counterfeit credit cards. Upgrading to EMV-ready point of sale terminals is the best way for business owners to protect themselves and their customers from this type of fraud.

ETA represents over 500 payments companies that collectively processed over $5 trillion in electronic payments last year. We represent acquiring banks, networks, payment processors, mobile carriers, fintech companies, and independent sales organizations. Our member companies work directly with merchants to enable access to the payments system and acceptance of their customers' preferred methods of payments.

ETA is the industry's trusted voice on educational efforts about the ongoing migration to chip cards. We have testified before the House Financial Services Committee and Small Business Committees in Congress, briefed state and federal regulators, and we recently sent your office helpful facts about chip cards to assist you in answering questions about chip cards from citizens of your state.

As you are also probably aware, a debate has developed that is unrelated to the chip card. The debate focuses on whether to impose a requirement that all eight million merchants and 1.2 billion payments cards be required to use a PIN as part of every transaction.

To be clear, a PIN isn't bad – in some cases, it can be beneficial – but a PIN isn't necessary for a chip card to serve its crime-fighting purpose. Put another way, the question of whether to implement chip cards, and the question of whether to deploy a nationwide PIN architecture, are two separate questions. Why? Because chip cards and PINs each address a different type of fraud at the check-out counter. Chip cards prevent counterfeit card fraud, which is currently two-thirds of all card fraud in stores in the U.S. PIN addresses lost and stolen cards, which represent about nine percent of in store fraud. That's why payments companies and merchants are currently prioritizing chip card deployment: chip cards cannot be counterfeited, and therefore chip cards stop the single largest category of card fraud in stores today.

So why not mandate PINs for every card transaction? Interestingly, such legacy customer verification methods are actually not required in most transactions in the U.S. today. Most electronic payments transactions in the U.S. -- 70% in fact -- currently require no PIN or signature. These transactions are generally low dollar amounts and carry very low risk of fraud, and thus allowing a consumer to "swipe and go" quickly through the checkout line is beneficial to consumers and merchants alike. Moreover, because two-thirds of all merchants don't

ELECTRONIC TRANSACTIONS ASSOCIATION

1101 16th Street NW
Suite 402
Washington, DC 20036

www.electran.org
T 800.695.5509
T 202.828.2635
F 202.828.2639

currently have a PIN pad, adding a PIN pad to the current chip migration efforts would add complexity and expense for merchants. Restaurants, for example, would have to reengineer the check out process entirely in order to allow customers at their tables to enter a PIN to pay. And today's popular mobile payments products use biometrics instead of PINs for customer verification, making a mandatory PIN infrastructure even less justifiable an investment.

ETA opposes government mandates of technology because mandates are a stationary target for fraudsters and limit incentives for the development of new technologies. Payments companies are currently deploying new customer verification technologies that will make static PINs obsolete, such as fingerprint, voice and face recognition. Any government mandate would force a reallocation of resources away from such promising innovations.

Importantly, during this entire migration to chip, consumers using cards remain 100 percent protected from any liability for fraud, regardless of whether or not a PIN is used in a chip transaction.

As you consider the question of whether to support a government mandate requiring that all merchants, banks and consumers must use PINs with chip cards, ETA urges you to carefully consider the investment and effort that financial institutions, payments companies, and merchants are making in chip card infrastructure. That investment is attacking the most fraud with the best technology available today to fight it. The PIN debate is important to many parties, but it should not interfere with the urgent work to stamp out counterfeit card fraud.

Please let me know if ETA or its members can be of any assistance to you in this, or any other payment matter.

Thank you,

Scott Talbott
Senior Vice President of Government Affairs
Electronic Transactions Association