New York Bankers Association

October 28, 2015

The Honorable Eric T. Schneiderman
Office of the Attorney General
The Capitol
Albany, New York 12224-0341

Re: Proposed "Chip & PIN" NAAG Letter

Dear Attorney General Schneiderman:

We understand that there is a NAAG letter being circulated that calls for all financial institutions to implement a static payment security technology, commonly known as Chip and PIN. The letter contains several mischaracterizations of security technology currently being deployed by the financial services industry. Additionally, the letter directly contradicts the official positions of all four federal bank regulators, including the Consumer Financial Protection Bureau. The static technology approach proposed in the letter not only fails to protect consumers now, but it makes Americans vulnerable to evolving financial fraud threats. On behalf of New York's diverse banks and credit unions operating under the watchful eye of state and federal regulators, **we urge you to either decline to sign this letter or withdraw your support if already given.** Anticipating your interest in a balanced view of this debate before endorsing the letter, we would like to share with you the following points:

- **This is not a consumer protection issue.** Consumers are protected by the zero liability protections offered by our industry.
- **With or without a PIN, it's the chip that matters.** The new EMV or "chip" cards generate a one-time code for each transaction, eliminating the possibility that stolen account numbers can be used to create counterfeit cards. The U.S. has already issued the most chip cards of any country in the world. Once chip cards fully replace the magstripe and merchants turn on their chip card readers, counterfeit cards will soon become a thing of the past.
- **PINs have nothing to do with data breaches.** PINs would not have prevented the data breaches at Target or Home Depot, and indeed, the impact of these breaches would have been magnified had massive numbers of PINs also been compromised. That scenario could have easily been the result if PINs were required on credit cards as some have advocated.

- **No technology is foolproof.** PINs have their own flaws. A report by the Federal Reserve Bank of Atlanta published in 2012 found that PIN debit fraud rates have increased more than threefold since 2004. Because a PIN is a static number that does not change, when a PIN is compromised, it can open a backdoor for criminals to access and drain consumers' bank accounts at an ATM.
- **Financial institutions are focused on the future, not the past.** Banks and credit unions annually spend billions on innovation in payment security in order to stay ahead of the thieves. Chips are part of the greater effort being made to combat thieves and hackers. Other innovations like tokenization (think Apple Pay or Samsung Pay) are becoming more common; they replace account numbers with a random number at the point of purchase, rendering them useless to thieves. Point-to-point encryption scrambles data at every point of the transaction. In addition to today's sophisticated neural networks that spot fraud at the point of sale, these new technologies will be layered on top of EMV and create multiple layers of security necessary to fight increasingly sophisticated forms of fraud. We don't know what thieves might do next—but that's exactly why mandating a static technology approach to security (such as PINs) is such a mistake.

As stated at the outset, these issues are complex policy matters in which we have sought and appreciated the input of Attorneys General. We are proud of our partnerships with law enforcement as we work together to fight financial crime. We would welcome the opportunity to discuss these issues further.

Thank you for the work you do.

Sincerely,

Michael P. Smith
President & CEO
New York Bankers Association

John J. Witkowski
President & CEO
Independent Bankers Association
of New York State

William J. Mellin
President & CEO
New York Credit Union Association