ROPES & GRAY

ALERT

Privacy & Data Security

December 4, 2015

State Attorneys General Fire Shot Across the Bow at Major Payment Card Brands Over "Chip and PIN" Technology

Attorneys

Heather Egan Sussman
Douglas H. Meal
James S. DeGraw
Seth C. Harrington
David McIntosh
Mark P. Szpak
Michelle Visser
Paul D. Rubin
Marc P. Berger
David T. Cohen

For well over a decade, U.S. regulators have been taking enforcement action against merchants and payment processors that, in the regulators' view, failed to take "reasonable and appropriate" steps to secure payment card information in their possession from the risk of unauthorized access by third-party criminals. No significant public regulatory pressure, however, was brought to bear on a key feature of the U.S. payment card system that incentivized criminals to steal that payment card information in the first place: the major payment card brands' failure to implement so-called "chip-and-PIN" technology that can substantially reduce criminals' ability to fraudulently use stolen payment card data.

This regulatory tolerance of the card brands' inaction may be waning. On November 16, 2015, Attorneys General from eight states (the "Attorneys General") sent a letter to leading payment card brands and banks that issue payment cards urging them to expedite the implementation of "chip-and-PIN" technology in the United States. Although the card brands and issuing banks have recently taken steps to promote the use of "chip-and-signature" cards, they did so only long after other developed countries had implemented chip technology. Moreover, the new "chip-and-signature" cards in the U.S., unlike the "chip-and-PIN" technology used abroad, are not designed to verify both the card and the individual using it. The Attorneys General argue that "there is no doubt" that chip-and-signature "is a less secure standard, since signatures can easily be forged or copied or even ignored at the point-of-sale."

As the Attorneys General note, "chip-and-PIN" has long been widely used for payment card transactions in Europe and other regions. According to EMVCo, 1.62 billion "chip-and-PIN" payment cards and 23.8 million terminals were in use globally by the close of 2012. *See* "Continued Marked Adoption of EMV Technology," EMVCo Newsletter, May 2013, available here. Within the United States, however, moves to adopt this technology have occurred much more slowly.

"Chip-and-PIN" requires the presence of both (1) a security chip embedded in the payment card that uses cryptography to protect payment card data; and (2) a user-selected personal identification number ("PIN") input by the user. "Chip-and-signature," by contrast, requires only the chip (and an easily forged signature). While the security chip provides enhanced protection against the use of counterfeit payment cards, it does not protect against the criminal use of cards that have been physically lost or stolen, among other things.

Both "chip-and-PIN" and "chip-and-signature" transactions require chip-enabled point-of-sale ("POS") terminals. The payment card brands have recently taken steps to encourage installation by merchants of POS terminals capable of accepting chip cards. Prior to October 1, 2015, card-present counterfeit fraud losses—losses caused by the use of a counterfeit payment card—were typically borne by the payment card issuer to the extent they were not reimbursed by a merchant that suffered a data breach or the bank that sponsored such merchant's participation in the payment system (known as an "acquiring" or "sponsoring" bank). As of October 1, 2015, if a merchant has not implemented chip-enabled point-of-sale technology, its acquiring bank must bear any card-present counterfeit fraud losses associated with use of a chip card at that merchant. The acquiring bank, in turn, may seek to hold the merchant responsible for such fraudulent transactions through its agreement with the merchant.

Additionally, payment card brands have recently implemented rules to incentivize merchants to transition to dual-interface, chip-enabled payment terminals by providing safe harbors from some liability in the event the merchant experiences a data breach. Those safe harbors may be available if the merchant, among other things, processes more than 95 percent of its card-present transactions with fully functional and operating chip-enabled terminals within designated periods of time. *See* MasterCard Security Rules and Procedures: Merchant Edition (July 31, 2014), at ¶ 10.2.5.4(b); Visa Global Compromised Account Recovery Guide: Visa Supplemental Requirements (January 2015), at 3. Dual-interface refers to payment terminals that can process chips both with and without direct contact with the chip. Additional requirements must be met, including that the merchant not have suffered a breach within the prior year.

The Attorneys General's letter recognizes these advancements, but cautions that they are too little, and too late. The letter takes the position that, as to chip technology, because "chip-and-PIN" is a known, more effective implementation for the protection of payment card data, and its adoption has proven to be feasible on a wide scale outside the U.S., the Attorneys General may consider the failure to adopt that implementation here unreasonable. The Attorneys General stopped short of suggesting that chip-and-PIN should actually be enshrined into law, noting they were sensitive to the concern that such enshrinement could pose risks to future innovation and/or give rise to incompatible technical requirements in different jurisdictions. But their letter cautions that the Attorneys General "cannot accept" the failure to implement chip-and-PIN in their jurisdictions, and that the card brands "can move more quickly to implement" it. The letter also draws a causal connection between recent major payment card breaches in the U.S. and the card brands' failure to implement chip-and-PIN. The letter notes that hackers have been "exploiting our continued reliance on outdated and less secure magnetic-stripe payment cards," and that the "U.S. has consistently accounted for about half of the global loss from fraudulent transactions, despite that it is responsible for only a quarter of total card payments." In short, the letter makes clear the Attorneys General's view that card brands and issuers "share in the responsibility for protecting the personal and financial information of their customers."

For more information regarding the Attorneys General's letter or the new "chip-and-signature" system, or to discuss data security practices generally, please feel free to contact Heather Sussman, Doug Meal, Jim DeGraw, Seth Harrington, David McIntosh, Mark Szpak, Michelle Visser, Paul Rubin, Marc Berger, David Cohen, or another member of Ropes & Gray's leading privacy & data security team.