BCLP. Client Intelligent

RetailLawBCLP

NEW SECURITY STANDARD FOR PINS WILL GIVE RETAILERS LESS COSTLY PROCESSING OPTIONS

Feb 09, 2018

A new standard published by the Payment Card Industry Security Standards Council ("PCI SSC") may make it easier and less costly for retailers to take advantage of lower cost PIN based transactions in card present scenarios. The new standard addresses security of PIN entry through software encryption solutions rather than only through hardware-based encryption devices.

The PCI Council's catchy name for this new standard is the PCI Software-Based PIN Entry on COTS (SPoC) Standard. "COTS" refers to Consumer Off-the Shelf devices, e. g., your iPhone or iPad or Android equivalents that are used as Mobile point-of-sale or "MPOS" purposes.

The primary purpose of the SPoC standard is to enable secure entry of PINS on tablets and mobile phones used to accept cards instead of the conventional POS terminals with dedicated PIN pads. The importance to retailers is that it may expand their ability to take advantage of lower cost processing options through mobile device acceptance channels.

The standard addresses at least two popular use cases. One is the familiar "Square" dongle on cell phones and another is the in-store mobile card entry devices that sales people use roaming around the stores. In the latter mode, devices utilizing the new standard will have to compete with existing mobile terminal devices that perform encryption within the hardware. These comply with the existing PCI PTS standard. These terminals have been in market for a while from several POS service providers. We don't know how the new SPoC compliant software devices will compare in merchant cost and security. A third case may be the tablet based card readers now appearing at POS counters.

You still need a PIN entry device under the new standard, but it can now be a dongle that meets the security standard. The standard may for example also find usage in the European-style restaurant payment devices. These mobile acceptance devices avoid the common USA scenario in which the server disappears with your card to produce a charge slip, doing who knows what else with your card while it is out-of-sight (the "Card Out of Sight" or "COoS" transaction – just kidding; that one is made up). That scenario is also addressed by existing hardware based mobile terminals that are beginning to appear. As the new methodology becomes more widely known, new applications may appear.

Retailers have a strong financial incentive to accept PIN-based debit card transactions from consumers because of the perceived lower costs associated with these payments. Since the Durbin Amendment imposed limits on debit card interchange fees and required that merchants be afforded alternative transaction routing options, PIN-based networks (Star, MAC, Pulse, NYCE, etc.) have an enhanced opportunity to compete as to payment processing costs, including the interchange fees that are passed to the issuer and the network processing costs. These costs are augmented by the merchant's processing fees as well, so the actual cost-effectiveness of PIN-based transactions varies considerably. Until the SPoC standard was published, there was no recognized secure software based method of accepting PINs in these alternative card entry devices.

The standard has four components but two will be the most burdensome. Those are detailed requirements for (i) a new software design standard, called the Secure Card Reader-PIN ("SCRP"); and (ii) a back office "active monitoring" procedural requirement. A major issue for the security of these devices is the secure management of encryption keys. The SPoC standard requires "perfect forward secrecy" and identifies one fairly old methodology, called Derived Unique Key per Transaction or "DUKPT" (pronounced duckputt) as one means for meeting that requirement. The inclusion of the monitoring function as a critical element of the standard tells us that PCI does not have a high enough level of confidence in the software solution alone.

The standard also requires secure software development and release practices to reduce compromise opportunities in those steps of the deployment process. The standard is limited to transactions entered as EMV chip-read or contactless card transmission (such as Near Field Communication ("NFC") or Samsung's proprietary Magnetic Secure Transmission ("MST"). The standard does not address security of PIN acceptance in eCommerce (online) or in-App sales channels.

It is not clear when compliant devices and supporting systems and service will be available for deployment. The announcement stated that test standards for third party validation of solutions would be published "later this year." PCI will also publish a list of validated systems, when available. This validation timetable effectively delays actual deployment, although it is likely that vendors have or will shortly have systems available that they believe will meet the standard that can be tested and priced for planning purposes. More information can be found on the PCI SSC website: https://www.pcisecuritystandards.org/pci_security/

For more information, contact the author, Stan Koppel, at 415-675-3437 or Stanton.Koppel@BryanCave.com, or any member of our Retail team.

RELATED PRACTICE AREAS

- Retail & Consumer Products

MEET THE TEAM

Merrit M. Jones

San Francisco

merrit.jones@bclplaw.com
+1 415 675 3435
