



April 15, 2009

Dear Sir/Madam:

The purpose of this letter is to encourage payment application vendors to validate their products to the Payment Card Industry Security Standards Council's (PCI SSC) Payment Application Data Security Standard (PA-DSS), formerly Visa's Payment Application Best Practices (PABP). Since the launch of PABP in 2004, 555 payment applications across more than 250 payment application vendors were independently validated by a Payment Application Qualified Security Assessor (PA-QSA). Visa continues to communicate with acquirers, processors, merchants, agents, payment application vendors and other key stakeholders to raise security awareness and drive the use of payment applications independently validated against PA-DSS and PABP.

Visa expects all payment application vendors' payment applications to adhere to the PA-DSS. The PA-DSS is designed to assist software vendors in creating secure payment applications, thereby helping to protect their customers from being exposed to a data security breach. The PA-DSS requirements prohibit the retention of sensitive authentication data including full magnetic-stripe (track) data, Card Verification Value 2 (CVV2) and PIN blocks—all critical impediments to achieving Payment Card Industry Data Security Standard (PCI DSS) compliance. Since 2007, Visa has worked with payment application vendors in identifying and listing vulnerable payment applications that retain sensitive authentication data post authorization. Vendors are encouraged to disclose vulnerabilities and remediation steps to their customers so immediate corrective action can be taken. As a practical matter, payment applications that do not meet PA-DSS may severely inhibit a merchant's or agent's ability to achieve compliance with the PCI DSS.

In the fall of 2007, Visa announced a series of payment application security mandates to eliminate the use of non-secure payment applications from the Visa payment system. These mandates require acquiring banks to ensure their merchants and agents do not use payment applications known to retain sensitive authentication data post authorization and require the use of payment applications that adhere to the PA-DSS requirements. PA-DSS compliant applications help merchants and agents mitigate compromises, prevent storage of prohibited data and support overall compliance with the PCI DSS.

Details on the PA-DSS program, validation and listing requirements are outlined on the PCI SSC website located at www.pcisecuritystandards.org along with information on the PCI DSS. Payment application vendors are strongly encouraged to list their products with the PCI SSC. Visa recommends that payment application vendors visit www.visa.com/cisp for specifics on Visa's payment application mandates and recent data security communications. Additionally, Visa holds PA-DSS training for payment application vendors throughout the year, which are published on the website.

Thank you in advance for your support. Visa encourages you to share this communication with your colleagues in the industry. Please contact cisp@visa.com should you have any questions.

Sincerely,

A handwritten signature in black ink, appearing to read "Eduardo Perez", is positioned above the typed name.

Eduardo Perez
Global Head of Data Security
Visa Inc.