



June 29, 2006

Dear Sir/Madam:

The purpose of this letter is to encourage payment application vendors to validate the conformance of their products to Visa's Payment Application Best Practices ("PABP"). Visa is augmenting its efforts to advance compliance with the Payment Card Industry Data Security Standard ("PCI DSS") by ensuring that payment applications used in the industry facilitate compliance. Visa is proactively encouraging all of its members, merchants and service providers to ensure that the payment applications they utilize are included on Visa's list of validated payment applications available at www.visa.com/cisp.

Visa developed the PABP to assist software vendors in creating secure payment applications, thereby helping to protect their customers from being exposed to a security breach. As stated in the PABP, Visa prohibits the retention of full magnetic-stripe ("track") data, Card Verification Value 2 ("CVV2") and PIN blocks—all critical impediments to achieving PCI DSS compliance. In addition to preventing the retention of prohibited data, the PABP requires payment applications to include security controls in support of a merchant or service provider's ability to comply with the PCI DSS.

Visa expects all payment application vendors to adhere to the PABP. As a practical matter, applications that do not meet PABP may inhibit merchant and service provider compliance with the PCI DSS. Visa is promoting its list of validated payment applications to all of its members, merchants and service providers. A number of Visa members and processors have already taken the proactive position of requiring all payment application vendors to have their products validated against the PABP as it is expected to soon become an industry standard requirement. Accordingly, Visa strongly encourages payment application vendors to validate the conformance of their products to the PABP. In addition, vendors must also provide instructions to all of their product's resellers and integrators on how to properly install PABP compliant software.

Details on the PABP program are outlined within the Visa Cardholder Information Security Program ("CISP") website at www.visa.com/cisp along with information on the PCI DSS. Visa encourages payment application vendors to review the PABP and engage a Qualified Payment Application Security Company to perform validation. Security assessors are included on the list of Qualified Data Security Companies found within the "Tools and FAQ" section of the CISP website. Payment applications validated against the PABP by a Qualified Payment Application Security Company will be included on Visa's list of validated payment applications on the CISP website.

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

Sincerely,

Eduardo Perez
Vice President
Payment System Risk and Compliance