Visa Issues Top 10 Best Practices for Payment Application Companies

September 3, 2010

Evolving threats to payment card data security and recent payment card data compromises have prompted Visa to issue a set of best practices for payment application companies to help mitigate security issues that lead to data compromises. Visa has recommended that acquirers, merchants, and agents should review Visa's best practices and insist that their payment application vendors, integrators, and resellers fully adopt the new standards. Visa's best practices recommend that payment application companies:

- Perform background checks on new employees and contractors prior to hire, including conducting investigations regarding previous employment history, academic history, credit history, and reference checks;
- Maintain an internal and external software security training and certification curriculum;
- Adhere to industry guidelines for data field encryption, tokenization, and PAN elimination across payment applications that use these technologies to help reduce risks to cardholder data;
- Adhere to a common software development life cycle based on ISO 12207 across payment applications to ensure that software is being properly developed and managed;
- Ensure that newly released payment application programs are compliant with the Payment Application Data Security Standard ("PA-DSS"); and
- Conduct application vulnerability detection tests and code reviews against common vulnerabilities and weaknesses prior to sale or distribution of payment application products to help companies identify and fix problems before the product release.

Visa noted that it has provided these standards to increase awareness of the payment application industry's best practices and stressed that all payment system participants should maintain compliance with the Payment Card Industry Data Security Standards ("PCI DSS"). The full list of Visa's best practices can be found here.