

AMERICAN BANKER®

THE FINANCIAL SERVICES DAILY

Wednesday, October 7, 2009

TECHNOLOGY

Visa Guidance on Data Encryption

■ BY DANIEL WOLFE

Visa Inc. has finally weighed in on the encryption debate, providing guidelines to merchants that choose to implement data security measures going beyond the industry-standard requirements.

Visa said earlier this year that it was exploring encryption technology, which some processors and terminal makers are already offering to merchants.

Encryption is not required under the Payment Card Industry data security standard, which describes how merchants must handle and protect card data. But the concept is getting more attention as companies realize that passing a PCI assessment may not be enough to prevent a data breach.

Eduardo Perez, Visa's global head of data security, said the encryption guidelines Visa announced Monday are meant to impress upon merchants that there is more to implementing encryption than buying any particular product.

"Encryption could be used to meet some of the requirements" under PCI, but

"encryption in and of itself is not a silver bullet," Perez said. "It should be taken seriously," so that the encryption keys, which can be used to decode scrambled files, are kept inaccessible, he said.

Encryption's most outspoken champion has been Heartland Payment Systems Inc. of Princeton, N.J., which began to advocate the technology after it disclosed a breach in January. Though it was later determined that Heartland had been out of compliance with the PCI standard, its security flaws were not revealed during numerous PCI assessments.

Heartland and other companies have begun to offer encryption options, or announced plans to do so, with a focus on "end to end" encryption. Typically, this means the data is encrypted when it is read by a merchant's terminal and remains encrypted until it has been handed off to the processor.

Visa accepts encrypted data, but only from merchants that are directly connected to its network. If a merchant is not a direct-connect client but its processor is,

the processor would have to decrypt the data as it comes in, and then encrypt it again before sending it to Visa.

Avivah Litan, a vice president and distinguished analyst at Gartner Inc., said Visa's new guidelines are broad enough to work with any existing encryption implementations. "It's not disruptive; it's complementary," she said.

However, she also said that offering broad guidelines rather than specific requirements "basically tells merchants there is ... not going to be an industry-wide end-to-end solution anytime soon."

Still, Visa's decision to issue a public statement may move some encryption efforts forward, Litan said. "This is a really useful announcement, because merchants may be sitting on the fence thinking, 'What's the card-brand position on this?'"

Rather than dictate specific technology, Visa is "basically separating" itself from the process while still providing some information for merchants that wish to seek its guidance, Litan said. ■