



Issue Date: CSP Daily News, January 13, 2009,

Visa Encryption Deadlines Loom

Requiring for debit card PINs on new pumps now, existing pumps by July 2010

SAN FRANCISCO -- Starting January 1, Visa Inc. is requiring all new fuel-dispensing machines being installed at gas stations around the United States to support the Triple Data Encryption Standard, a mandate that is designed to make it harder for identity thieves to steal debit card data from gasoline pumps by shielding the personal identification numbers (PIN) of customers. Card-skimming devices placed on gasoline dispensers have been used to compromise payment card data, said *Computerworld*.

Visa's new requirement calls on gasoline retailers to ensure that all new pumps capable of processing debit card purchases are equipped with an encrypting PIN pad, or EPP, that supports Triple DES, according to the publication. Although Visa is the only credit-card company mandating the use of the encryption technology now, the requirement is expected to become part of a broader specification for unattended point-of-sale (POS) systems that is being developed by the PCI Security Standards Council, which is responsible for the Payment Card Industry Data Security Standard and other data protection measures.



- ADVERTISEMENT -



Station owners have until July 1, 2010, to ensure that all of their existing pumps are upgraded to support Triple DES. Robert Renke, executive vice president of the Petroleum Equipment Institute (PEI), estimated that about 1.4 million gasoline pumps would need to be retrofitted with new software, for an average of more than 2,500 per day in order for retailers to meet Visa's deadline.

The chances of that happening are remote, according to some analysts. The upgrade requirement is "a major deal for gas stations with old equipment," Gartner Inc.'s Avivah Litan told the magazine. And with the down economy and drivers cutting back on fuel consumption after prices hit record levels last summer, "this could not come at a worse time for gas station operators," she added. "I'm sure many will be late when it comes to compliance."

She said that if an existing gasoline dispenser cannot support a software upgrade to make it compliant with Triple DES, a replacement pump may have to be installed. And on top of the encryption requirements, stations will need to ensure that the POS systems on their pumps comply by July 2010 with a separate payment application security standard that was crafted by Visa and then adopted by the PCI council. Full replacements can cost between \$8,000 and \$29,000 per pump, Litan said.

Retailers that only need to upgrade their existing pumps can expect to spend between \$1,800 and \$2,000 per card reader, Renke said. But he added that given the razor-thin profit margins and fiercely competitive environments that most station owners face, investing even that much money in the security upgrades will be a major challenge for many.

"This is going to be a huge undertaking," Jim Huguelet, an independent PCI consultant in Bolingbrook, Ill., told the magazine. Between 20% and 30% of gasoline purchases made at the pump are processed via PIN-based debit transactions, he said. He noted that stations that cannot or are unwilling to make the required investments in pump upgrades or replacements may have to stop accepting such transactions next year.

The new data encryption requirements for stations are part of a wider effort, started by Visa five years ago, to enforce tougher security standards on self-service gasoline pumps, ATMs, retail kiosks and other unattended POS systems, as well as PIN entry devices that are monitored by employees at a retailer or other merchant.

According to a [document](#) that Visa issued in September to outline the Triple DES requirements, a complete conversion to the encryption technology on POS devices will require upgrades to systems and networks at banks and payment processing firms in addition to the ones at gas stations and other merchants.

The PCI Security Standards Council announced plans in August to add security requirements for unattended POS systems that all entities accepting payment card transactions via such devices will need to comply with. A draft of the requirements has already been published for review, and council members have submitted comments about the draft. A final version is expected to be released sometime this year, said the report.

[Click here](#) to view *CSP* magazine's cover story on data security.