Is Your Business Visa CISP Compliant?

Your Customers' Security = Security For Your Business!

The Federal Trade Commission's Consumer Fraud and Identity Theft Complaint Data report stated that credit card fraud was the most common form of reported identity theft in 2005 at 26%.
"Consumer Fraud and Identity Theft Complaint Data" Federal Trade Commission report, January 25, 2006.

Joe Majka, Vice President of Fraud Control at Visa says, "Criminals want the data that is on the card's magnetic stripe. The majority of data security breach incidents reported to Visa have involved retail merchants."
"Putting the Squeeze on Credit Card Fraud" by Joris Evers, Staff Writer, CNET News.com, September 9, 2005.

Surveys in the USA from July, 2003 to January, 2006 showed an increase in the total value of identity fraud to $56.6 billion in 2006. The average fraud per person rose from $5,249 in 2003 to $6,383 in 2006.
Recent Surveys and Studies, Privacy Clearing House, Wikipedia.org, June 30, 2006.

The 2003 survey from the *Identity Theft Resource Center* found that:

- Only 15% of victims find out about the theft due to a proactive action taken by a business.
- The average time spent by victims resolving the problem is about 600 hours.
- 73% of respondents indicated the crime involved the thief acquiring a credit card.
- The emotional impact is similar to that of victims of violent crime.

Regarding the sensitive information encoded in the magnetic stripe on credit cards, John Shaughnessy, Senior Vice President for Risk Management at Visa USA, says these secret codes are "jewels" for thieves. "The fact that it's stored anywhere is troublesome."
"Stores Blame Checkout Software for Security Breaches" by David Bank, Staff Reporter, Wall Street Journal, April 27, 2005.

Visa's Card Information Security Program (CISP) initiative is in place to protect Visa cardholder data–wherever it resides–ensuring that members, merchants, and service providers maintain the highest information security standard. MICROS has followed Visa's lead by implementing changes to all of its PMS/POS applications to prevent the storage of full magnetic stripe data. ***MICROS is a Visa USA Payment Application Best Practices technology provider.***

We know that you support Visa's goal in protecting customers from potential credit card fraud and identity theft, so as your technology partner, we are wholly committed in supporting you with becoming compliant with Visa CISP.

Factors to Consider:

- The Payment Card Industry Data Security Standard (PCI DSS) mandates that all merchants accepting the Association's (Visa, MasterCard, American Express and Discover) card brand must adhere to this standard in order to continue accepting credit cards. *http://usa.visa.com*

Visa has the authority to:

- Penalize the merchant $100,000 per incident for failure to immediately notify Visa USA Fraud Control of the suspected or confirmed loss or theft of any Visa transaction information.
- Fine the merchant up to $500,000 per incident if compromised and not compliant at the time of the incident.
- PERMANENTLY prohibit the merchant from participating in Visa programs, if they are not in compliance with the security requirements or fail to rectify a security issue.

Katie Jenkins, Principal Consultant with VeriSign Inc., says, "If found to be non-compliant, merchants may be fined or Visa could impose restrictions on a merchant (up to not being able to accept Visa payments). Egregious violations (i.e. breach of track data) can be up to $500,000. Plus members incur costs like forensics investigations if there is a compromise (not to mention damage to reputation, etc)."

Delays in becoming CISP compliant could negatively impact your reputation, customer welfare, and ultimately your business.

micros®

How can you ensure that your MICROS Systems are compliant?

Step 1: *Contact your local MICROS office or account manager to detemine if you need to upgrade the MICROS software you are utilizing.*

Step 2: *Schedule an appointment with MICROS to have your systems upgraded.*

MICROS Validated Products:

MICROS Restaurant POS Products

- *9700 HMS Version 3.0 +*
- *RES 3000 (3700) Version 4.0 +*
- *RES 3000 (3700) Version 3.2 (SP7HF5) with Merchant Link Transaction Vault*
- *MICROS e7 Version 2.11 +*
- *Simphony Version 1.0*

MICROS - Retail POS Products

- *Datavantage Store21 Version 4.68 +*
- *Datavantage TradeWind Version 8.7 +*
- *Datavantage Xstore Version 1.00.63.4 +*
- *Datavantage DAS Version 2.0.2.1*
- *Datavantage TradeCipher Version 1.01.0140*
- *Datavantage Xpay Version 1.01.50*
- *Datavantage Xsettlement Version 2.0*
- *CW Direct Version 10.0*

Hotel Software Products

- *OPERA Property Management System V3.6+*
- *Fidelio Version 8.6.05*

PCI Data Security Standard

Build and Maintain a Secure Network	1. Install and maintain a firewall configuration to protect data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored data 4. Encrypt transmission of cardholder data and sensitive information across public networks
Maintain a Vulnerability Management Program	5. Use and regularly update anti-virus software 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to data by business need-to-know 8. Assign a unique ID to each person with computer access 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security

For more information about Visa CISP, contact AskVisaUSA@Visa.com or contact your local MICROS Account Manager