

CARD PAYMENT SECURITY

Payment Card Industry (PCI) Data Security Standards &
Visa U.S.A. Cardholder Information Security Program (CISP)



DSW Customers Warned About Security Breach *More Customers Affected Than Originally Thought*

April 19, 2005

MORE CUSTOMER DATA MISSING

Retail Ventures and Ameritrade report data mishaps, but a new standard backed by credit-card companies could raise the bar on data protection

By Steven Marlin, InformationWeek, April 25, 2005

Theft of Credit Card Info from Polo Ralph Lauren Hits Thousands

Breach affects 180,000 Mastercard holders; breach was first known about in January

Associated Press, April 14, 2005

“Millions of consumers have been exposed to potential identity theft in 14 major breaches in the past year.”

Washington Post, April 13, 2005

IN THIS AGE OF HEIGHTENED SECURITY CONCERNS, ALOHA IS COMMITTED TO PROVIDING OUR CLIENTS WITH SOLUTIONS THAT ASSIST THEM IN AVOIDING FINANCIAL AND REPUTATIONAL LOSSES AS WELL AS SAFEGUARD THEIR CUSTOMERS' INFORMATION. IN A PROACTIVE EFFORT TO UPHOLD CONSUMER CONFIDENCE IN THE SECURITY OF THE ALOHA PRODUCT, ALOHA HAS SUCCESSFULLY RECEIVED VALIDATION WITH VISA U.S.A.'S PAYMENT APPLICATION BEST PRACTICES FOR THE ALOHA VERSION 5.3.15 THROUGH VISA'S CARDHOLDER INFORMATION SECURITY PROGRAM (CISP).

CISP DEFINES A STANDARD FOR SECURING VISA CARDHOLDER DATA WHEREVER IT IS LOCATED. CISP COMPLIANCE IS REQUIRED OF ALL ENTITIES THAT STORE, PROCESS OR TRANSMIT VISA CARDHOLDER DATA. CISP COMPLIANCE REDUCES THE RISK OF FRAUD AND PROVIDES A SAFER, MORE SECURE PROCESSING ENVIRONMENT FOR YOU AND YOUR CREDIT AND DEBIT CARD CUSTOMERS. MERCHANTS WHO ARE NOT COMPLIANT WITH CISP REQUIREMENTS POSE A GREATER RISK OF CREDIT CARD FRAUD AND COULD BE SUBJECTED TO SANCTIONS FROM VISA.



WHAT ALOHA PRODUCT IS VALIDATED?

Aloha POS version 5.3.15 has been verified against the PCI Data Security Standards and Visa CISP Best Practices by an independent third party.

WHO DOES CISP APPLY TO?

CISP compliance is required of all entities that store, process or transmit Visa cardholder data.

ALOHA ALIGNS WITH PCI STANDARDS THROUGH PRODUCT ENHANCEMENTS

Visa U.S.A. has accepted Radiant Systems' CISP Payment Application Validation for Aloha Suite version 5.3.15 application, based on the assessment and opinion of Ambiron LLC.

FOR MORE INFORMATION

To learn more about the Visa CISP, contact Visa via email at AskVisaUSA@Visa.com



THE PAYMENT CARD INDUSTRY (PCI) DATA SECURITY STANDARDS IS A RESULT OF COLLABORATION BETWEEN THE VARIOUS CREDIT CARD ASSOCIATIONS AND THE FEDERAL GOVERNMENT TO CREATE COMMON INDUSTRY SECURITY REQUIREMENTS. EACH CARD ASSOCIATION STILL MAINTAINS THEIR OWN PROGRAM IDENTITY NAME, FOR INTERNAL PURPOSES WITHIN THEIR OPERATING RULES AND REGULATIONS, SUCH AS VISA CISP, MASTERCARD SDP (SITE DATA PROTECTION), ETC. HOWEVER THEY ARE GENERALLY REFERRED TO IN A COMMON LANGUAGE AS THE REQUIREMENTS OF "THE PCI STANDARDS."

PCI DATA SECURITY STANDARD

Using the PCI Data Security Standard as its framework, CISP provides the tools and measurements needed to protect against cardholder data exposure and compromise across the entire payment industry. The PCI Data Security Standard consists of 12 basic requirements supported by more detailed sub-requirements:

PCI DATA SECURITY STANDARD	
Build and Maintain a Secure Network	<ul style="list-style-type: none"> ▶ Install and maintain a firewall configuration to protect data ▶ Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	<ul style="list-style-type: none"> ▶ Protect stored data ▶ Encrypt transmission of cardholder data and sensitive information across public networks
Maintain a Vulnerability Management Program	<ul style="list-style-type: none"> ▶ Use and regularly update anti-virus software ▶ Develop and maintain secure systems and applications
Implement Strong Access Control Measures	<ul style="list-style-type: none"> ▶ Restrict access to data by business need-to-know ▶ Assign a unique ID to each person with computer access ▶ Restrict physical access to cardholder data
Regularly Monitor and Test Networks	<ul style="list-style-type: none"> ▶ Track and monitor all access to network resources and cardholder data ▶ Regularly test security systems and processes
Maintain an Information Security Policy	<ul style="list-style-type: none"> ▶ Maintain a policy that addresses information security

Source: <http://usa.visa.com>



FOR MORE INFORMATION, PLEASE VISIT US AT
WWW.RADIANTSYSTEMS.COM OR CONTACT US AT 800.229.0991 x8000

▶ ATLANTA ▶ DALLAS ▶ MELBOURNE ▶ PRAGUE ▶ SINGAPORE