CISP BULLETIN

Visa Alerts Acquirers to Payment Applications That Store Sensitive Cardholder Data

July 1, 2008

It has been brought to Visa's attention that certain payment applications are designed to store sensitive cardholder data — including full magnetic-stripe, Card Verification Value 2 (CVV2) or PIN data — following transaction authorization. Storage of this type of data is in violation of the Payment Card Industry (PCI) Data Security Standard (DSS) and the *Visa U.S.A. Inc. Operating Regulations*. It is critical that acquirers (i) ensure that their merchants and agents do not use payment applications known to retain sensitive cardholder data elements; (ii) take corrective action to address any identified deficiencies; and (iii) insist that their merchants and agents use payment applications that have been validated against Visa's Payment Application Best Practices (PABP). A list of validated applications is available at www.visa.com/cisp.

Payment Applications Storing Sensitive Cardholder Data

Payment applications often store sensitive cardholder data post-authorization without the merchant's or agent's knowledge. Acquirers, merchants and agents should ask their payment application vendors (or resellers and integrators) to confirm that their software does not store magnetic-stripe data, CVV2 data, PINs or encrypted PIN blocks. This information can be verified by asking the payment application vendor to disclose a list of files written by the application and share a summary of the contents of those files. Acquirers, merchants and agents must confirm that all cardholder data storage is necessary and appropriate for the transaction type.

It is critical for acquirers to ensure that merchants and agents using these applications take appropriate action to eliminate sensitive cardholder data from being stored on their systems. To assist with this process, Visa has compiled the following list of applications that have been identified as storing full magnetic-stripe data. In some cases, the product vendor has provided a recommended fix to address the magnetic-stripe data issue; these product versions or patches are also noted. If a PABP-validated product version of the application is available, it is noted as well.

Updates to this list will be made periodically, and changes may be made to the listing of products that affect Visa's views. *This list is not to be published publicly; however, acquirers may share this list with their merchants and agents. When sharing this list, acquirers must not publish the list to a website or to a place where the list may be made publicly available.* For detailed information about these products and their respective fixes or upgrades, please contact the product vendors directly.

The information provided herein is provided "AS IS," with no warranties, expressed or implied, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose and / or non-infringement. The information provided in this bulletin is subject to change by Visa, with or without notice. Although Visa makes good faith efforts to provide accurate and complete information, merchants (or anyone else using the information set forth on the following

list) remain responsible for confirming the accuracy of this information, including, but not limited to, confirming with the appropriate payment application vendor whether the version of the application identified below stores sensitive authentication data (i.e., magnetic-stripe data, CVV2 data, PINs or PIN blocks) and is in compliance with PABP. Use of any one or more of the applications below does not guarantee or ensure compliance with the PCI DSS and does not satisfy acquirers' obligation to perform their own evaluation and due diligence to ensure the PCI DSS compliance of their merchants and agents.

As they are identified, Visa will share with acquirers the names of any additional payment applications that may retain sensitive cardholder data.

PAYMENT APPLICATION VENDOR	DATE PUBLISHED	PRODUCT VERSION THAT MAY RETAIN MAGNETIC-STRIPE DATA	PRODUCT VERSION/PATCH THAT DOES NOT RETAIN MAGNETIC-STRIPE DATA	PABP-VALIDATED PAYMENT APPLICATION
Affiliated Computer Services, Inc. www.acs-inc.com	July 2007	WebPRCS All versions prior to v7.0	WebPRCS v7.0+	
	July 2007	Omnimatic v3.1		
	July 2007	Omnimatic v2.1		
	July 2007	PRCS – TIM All versions prior to v4.0	PRCS – TIM v4.0+	
			WebPRCS v7.0+	
	July 2007	PRCS – PC All versions prior to v6.1	PRCS – PC v6.1+	
			WebPRCS v7.0+	
AutoGas www.autogas.com	October 2007	AutoGas REGAL All versions prior to Streamline 2 v4.10	AutoGas REGAL Streamline 2 v4.10	AutoGas REGAL Streamline 2 v4.10
CAM Commerce Solutions www.camcommerce.com	January 2008	Profit$ All versions prior to v3.5 release 9	Profit$ v3.5 release 9 and later	
Comdata www.comdata.com	October 2007	Trendar All versions prior to v617	Trendar v617	
Emporos Systems www.emporos.net	January 2008	MerchantSoft POS v7.0.0.3c	MerchantSoft POS v7.0.0.6xml	
Excentus www.excentus.com	October 2007	Reward Fuel Controller All versions prior to v3.0	Reward Fuel Controller v3.0	
Focus POS Systems, Inc. www.focuspos.com	October 2007	Focus POS All versions prior to v6.11.23	Focus POS v6.11.23	Focus v7.4
Gilbarco Veeder-Root www.gilbarco.com	October 2007 May 2008 (update)	Passport All versions prior to v6.00.xx	*Customers who are operating the versions listed should contact Gilbarco to obtain upgrades*	Passport (Concord/First Data) v6.00.23.02
				Passport (Chevron) v6.00.26.02

PAYMENT APPLICATION VENDOR	DATE PUBLISHED	PRODUCT VERSION THAT MAY RETAIN MAGNETIC-STRIPE DATA	PRODUCT VERSION/PATCH THAT DOES NOT RETAIN MAGNETIC-STRIPE DATA	PABP-VALIDATED PAYMENT APPLICATION
				Passport (Exxon Mobil) v6.00.28.02
	October 2007	G-SITE ADS – Chicago All versions prior to v22.1.0.3		
	October 2007	G-SITE Concord/Buypass All versions prior to v6.4.03		
HotSauce Technologies www.hotsaucepos.com	October 2007 May 2008 (updated)	HotSauce Restaurant Management Solutions (RMS) All versions prior to v5.9.6.1	HotSauce Restaurant Management Solutions (RMS) v5.9.6.1+	
	July 2007	EVS v1	EVS v2+	
IBM www.ibm.com	October 2007	ACE Electronic Payment Support (EPS) v6 All levels prior to S106	ACE Electronic Payment Support (EPS) v6 Level S106 and later	
	October 2007	ACE Electronic Payment Support (EPS) v5 All levels prior to P150	ACE Electronic Payment Support (EPS) v5 Level P150 and later	
	October 2007	ACE Electronic Payment Support (EPS) v4 All levels prior to N166	ACE Electronic Payment Support (EPS) v4 Level N166 and later	
	October 2007	ACE Electronic Payment Support (EPS) v3 All levels prior to M207	ACE Electronic Payment Support (EPS) v3 Level M207 and later	
	July 2007	StorePay All versions prior to v5.0	StorePay v5.0+	
ICVERIFY, Inc. www.icverify.com	April 2007	ICVERIFY for Windows v2.x (produced by CyberCash, Inc. prior to 2002)	ICVERIFY for Windows v3.x	ICVERIFY for Windows v4.0.3
			ICVERIFY for Windows v2.x Service Pack 1 (available since 2003)	ICVERIFY for Windows v4.0 (available since 2005)
Integrated Business Systems, Inc. www.goibs.com	July 2007	Club Management System v6.42.0.0	Club Management System v6.6+	

PAYMENT APPLICATION VENDOR	DATE PUBLISHED	PRODUCT VERSION THAT MAY RETAIN MAGNETIC-STRIPE DATA	PRODUCT VERSION/PATCH THAT DOES NOT RETAIN MAGNETIC-STRIPE DATA	PABP-VALIDATED PAYMENT APPLICATION
ISD Corporation www.isdcorporation.com	July 2007	Message Sentry v1 for iSeries	Payment Switch Framework Authorization & Settlement Suite v6.x for JAVA or v5.1+	Payment Switch Framework Authorization & Settlement Suite v6.0 for JAVA
	July 2007	Message Sentry v1 for UNIX		Payment Switch Framework Authorization & Settlement Suite v5.2
	July 2007	Message Sentry v1 for Mainframe	See v5.x for iSeries or UNIX See v6.x for JAVA	Payment Switch Framework Authorization & Settlement Suite v5.1
	July 2007	Payment Switch Framework Authorization & Settlement Suite v1.0	Payment Switch Framework Authorization & Settlement Suite v6.x	
MenuSoft www.digitaldining.com	April 2007	Digital Dining All versions using a DDServ.dll file prior to v7.3.0350	Digital Dining All versions using a later DDServ.dll file to and including v7.3.0350	Digital Dining v7.3.04
				Digital Dining v7.3.03
Micros www.micros.com	April 2007	8700 HMS v2.70 through v2.70.14 *	8700 HMS v3.00	
			8700 HMS v2.70.15+	
	April 2007	8700 HMS v2.50 through v2.50.20 *	8700 HMS v2.50.21+	
	April 2007	8700 HMS v2.11.0 through v2.11.9 *	8700 HMS v2.11.10+	
	April 2007	8700 HMS v1.00 through v2.10		
	April 2007 May 2008 (updated)	9700 HMS All versions prior to v2.50	9700 HMS All later versions to and including v2.50 *	9700 HMS v3.2
				9700 HMS v3.1
				9700 HMS v3.0 Service Pack 6 through 12
	April 2007	RES 3000 v3.2.0 *	RES 3000 v3.2.1+	RES 3000 v4.1
	April 2007	RES 3000 v3.1.0 *	RES 3000 v3.1.3+	RES 3000 v4.0.17.502
	April 2007	RES 3000 v1 through v3.0		
Multi-Systems, Inc. www.msisolutions.com	July 2007	WinPM v1.90	WinPM v1.95	
	July 2007	WinPM v1.80		
	July 2007	WinPM v1.63		

PAYMENT APPLICATION VENDOR	DATE PUBLISHED	PRODUCT VERSION THAT MAY RETAIN MAGNETIC-STRIPE DATA	PRODUCT VERSION/PATCH THAT DOES NOT RETAIN MAGNETIC-STRIPE DATA	PABP-VALIDATED PAYMENT APPLICATION
	July 2007	WinPM v1.62		
NCR www.ncr.com	July 2007	ScanMaster All 2.1.xx.xx versions prior to v2.01.00.30	Advanced Checkout Solution (ACS) v6.0+	Advanced Checkout Solution (ACS) v6.02.01
	July 2007	ScanMaster All 2.0.xx.xx versions prior to v2.00.03.12		Advanced Checkout Solution (ACS) v6.00.10
	July 2007	ScanMaster All 1.2.xx.xx versions prior to v1.2.3.26		Advanced Checkout Solution IR (ACS-IR) v6.01.04
	July 2007	ScanMaster v1.1.6.xx		
osCommerce www.oscommerce.com	January 2008	osCommerce v2.1		
Posera www.posera.com	April 2007	Maitre'D All later versions prior to v2005 Service Pack 3	Maitre'D All later versions to and including v2005 Service Pack 3	Maitre'D v2005 Service Pack 3
	April 2007	Maitre'D All versions prior to v2003 Service Pack 11	Maitre'D All later versions to and including v2003 Service Pack 11	Maitre'D v2003 Service Pack 11
	April 2007	Maitre'D All versions of v2002		
Postilion (S1 Corporation) www.postilion.com	May 2008	Realtime Framework All versions prior to v4.2 Service Pack 3	Realtime Framework All later versions to and including v4.2 Service Pack 3	Realtime Framework v4.3
Radiant Systems www.radiantsystems.com	April 2007	Aloha Suite All versions prior to v5.3.15	Aloha Suite All later versions to and including v5.3.15	Aloha Suite v6.1
				Aloha Suite v5.3.15
Southern DataComm www.protobase.com	April 2007	ConnectUp All versions	ProtoBase® v4.83.xx	ProtoBase® v6.01
	April 2007	PopsOn All versions	ProtoBase® v4.82.xx	ProtoBase® v6.0
	April 2007	ProtoBase® v4.80.xx	ProtoBase® v4.81.xx	
	April 2007	ProtoBase® v4.7x.xx		
	April 2007	PBAdmin® v5.00.xx	PBAdmin® v5.02.xx	
	April 2007	PBAdmin® v4.01.xx	PBAdmin® v5.01.xx	

PAYMENT APPLICATION VENDOR	DATE PUBLISHED	PRODUCT VERSION THAT MAY RETAIN MAGNETIC-STRIPE DATA	PRODUCT VERSION/PATCH THAT DOES NOT RETAIN MAGNETIC-STRIPE DATA	PABP-VALIDATED PAYMENT APPLICATION
VeriFone, Inc. www.verifone.com	January 2008	Ruby PTIPAK (Chase Paymentech) All versions prior to v4.00 – Base 161 PABP	Ruby PTIPAK (Chase Paymentech) v4.00 – Base 161 PABP	Ruby PTIPAK (Chase Paymentech) v4.00 – Base 161 PABP
	July 2007	Ruby, Topaz Buypack (First Data) v4.01.xx	Ruby Buypack (First Data) v4.08.xx	
	July 2007	Ruby, Topaz Buypack (First Data) v2.10.xx	Topaz Buypack (First Data) v4.09.xx	
	July 2007	Ruby, Topaz Buypack (First Data) v2.09.xx		
	July 2007	Ruby, Topaz Buypack (First Data) v2.08.xx		
	July 2007	Ruby, Topaz *(Store & Forward Fleet and Debit)* Buypack (First Data) v4.07.xx		
	July 2007	Ruby, Topaz *(Store & Forward Fleet and Debit)* Buypack (First Data) v4.06.xx		

* For the noted Micros applications, third-party solutions developed by Shift4 and Merchant Link may support a merchant's PCI DSS compliance. These third-party solutions may or may not be endorsed / created by the original product vendor. Please refer to the list of Validated Payment Applications at www.visa.com/cisp and contact the product vendors for more information.

Visa Champions PCI DSS and PA-DSS Compliance

Visa is working with all key stakeholders — acquirers, processors, merchants, agents and payment application vendors — to raise security awareness and encourage the use of payment applications that support PCI DSS compliance. In April 2008, the PCI Security Standards Council (SSC) adopted Visa's PABP and released the standard as the Payment Application Data Security Standard (PA-DSS). To promote proactive compliance with the PA-DSS, Visa is communicating directly with software vendors to help them better understand the value of PA-DSS compliance and to encourage them to validate the conformance of their products to the PA-DSS.

On January 1, 2008, Visa also implemented a series of U.S. mandates to eliminate the use of non-secure payment applications from the Visa payment system. These mandates require acquirers to ensure that their merchants and agents do not use payment applications known to retain sensitive cardholder data elements and call for the use of payment applications that adhere to the PABP (now PA-DSS). Accordingly, as of January 1, 2008, newly boarded merchants must not use known vulnerable payment applications, and VisaNet Processors (VNPs) and agents must not certify new payment applications to their platforms that have been identified as vulnerable payment applications.

Acquirers Can Minimize Data Security Risks by Promoting PA-DSS Validation

Merchants and agents may mistakenly believe that they need to store prohibited elements of track data for certain types of transactions; however, acquirers should ensure that merchants have established proper processes for each type of transaction so that sensitive cardholder data is not retained. Storage of the following magnetic-stripe data elements **is permitted:** cardholder's name, primary account number, expiration date and service code. These values, which should be stored only if needed to perform business functions, must be protected in accordance with the PCI DSS.

Acquirers must ensure that merchants or agents using applications that store sensitive cardholder data upgrade to a version that does not retain sensitive data. This may be accomplished by implementing an updated application version or patch made available by the vendor or by selecting an alternative PABP-validated application. In addition to upgrading the application, any historical storage of full track data must be securely wiped from all systems immediately. A secure wipe utility should be obtained from the software vendor or a third-party vendor.

By July 1, 2008, VNPs and agents must certify to their platforms only those new payment applications that are PABP-compliant.

To view the list of more than 300 payment applications already validated against the PABP, visit the Visa Security Compliance website at www.visa.com/cisp. In late 2008, the PCI SSC will assume management of this list.

For more information on Visa's compliance programs, please visit http://www.visa.com/cisp. Questions about this bulletin may be directed to CISP@visa.com.