



Visa Communication Alert

Payment Applications that Store Prohibited Data

August 10, 2007

This communication alert provides important information for acquirers, VisaNet processors, third-parties (Independent Sales Organizations, Third Party Service Providers and Merchant Servicers), law enforcement agencies, software vendors and other key stakeholders regarding payment applications that store prohibited cardholder data. The payment applications listed in this alert have been identified as storing full magnetic stripe data in violation of the *Visa U.S.A. Inc. Operating Regulations* and Visa's Payment Application Best Practices (PABP).

This is a call to action for all acquirers, VisaNet processors and third parties to drive merchant adoption of PABP-validated applications, and to ensure merchants using the applications noted below take corrective action to address any identified deficiencies.

Additionally, Visa will host three conference calls to discuss this topic, as listed at the end of this alert.

Storage of Prohibited Data by Payment Applications

It has been brought to Visa's attention that certain payment applications are designed to store prohibited data subsequent to transaction authorization in violation of the PCI DSS and the *Visa U.S.A. Inc. Operating Regulations*. Hackers, who know that many merchant systems store prohibited data, are targeting agents and merchants using vulnerable payment applications, and exploiting vulnerabilities to find and steal this data.

The following applications have been identified as storing full magnetic stripe data. In some cases, the product vendor has provided a recommended fix for the application to address the magnetic-stripe data issue, and these product versions or patches are noted below. If a PABP-validated product version for the application is available, it is also noted below. It is critical that merchants and agents using these applications take appropriate action to eliminate prohibited data from being stored on their systems.

Please be advised that Visa makes no endorsement of applications or products, or each of their respective developers or distributors, and disclaims all warranties expressed or implied. Updates to this list will be made periodically, and changes may be made to products that affect Visa's views. *This list is not to be published publicly.* For more detailed information about these products and their respective fixes / upgrades, please contact the product vendors directly.

Payment Application Vendor	Product Version that May Retain Magnetic Stripe Data	Product Version/Patch that Does Not Retain Magnetic Stripe Data	PABP-Validated Product Version
Affiliated Computer Services, Inc.	Omnimatic V2.1, V3.1	WebPRCS V7.0+	
	PRCS – TIM	PRCS – TIM	



Payment Application Vendor	Product Version that May Retain Magnetic Stripe Data	Product Version/Patch that Does Not Retain Magnetic Stripe Data	PABP-Validated Product Version
	All versions prior to V4.0	V4.0+ WebPRCS V7.0+	
	PRCS – PC All versions prior to V6.1	PRCS – PC V6.1+ WebPRCS V7.0+	
	WebPRCS All versions prior to V7.0	WebPRCS V7.0+	
HotSauce Technologies	EVS V1	EVS V2+	
IBM	StorePay All versions prior to V5.0	StorePay V5.0+	
ICVERIFY, Inc.	ICVERIFY Software for Windows V2.X (produced by CyberCash, Inc. prior to 2002)	ICVERIFY Software for Windows V2.X Service Pack 1 (available since 2003) ICVERIFY Software for Windows V3.X	ICVERIFY Software for Windows V4 (available since 2005)
Integrated Business Systems, Inc.	Club Management System V6.42.0.0	Club Management System V6.6+	
ISD Corporation	Message Sentry V1 for iSeries	Payment Switch Framework Authorization & Settlement Suite V5.1+ or V6.x for JAVA	Payment Switch Framework Authorization & Settlement Suite V5.1, V5.2
	Message Sentry V1 for UNIX		
	Message Sentry V1 for Mainframe	See V5.x for iSeries or UNIX See V6.x for JAVA	V6.x for JAVA
	Payment Switch Framework Authorization & Settlement Suite V1.0	Payment Switch Framework Authorization & Settlement Suite V6.x	
MenuSoft Systems	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 V7.3.0375
Micros Systems, Inc.	8700 HMS V1.00 thru V2.11.9	8700 HMS V2.11.10+	
	V2.50 thru V2.50.20	V2.50.21+	
	V2.70 thru V2.70.14	V2.70.15+ V3.00	



Payment Application Vendor	Product Version that May Retain Magnetic Stripe Data	Product Version/Patch that Does Not Retain Magnetic Stripe Data	PABP-Validated Product Version
	9700 HMS All versions prior to V2.50	9700 HMS All later versions to and including V2.50	9700 HMS V3.0 service pack 6 thru 12 and HMS V3.1
	RES 3000 V1 thru V3.1.2 V3.2.0	RES 3000 V3.1.3 + V3.2.1 +	RES 3000 V4.1, 4.0 and V3.2 service pack 7 hotfix 5 with TransactionVault
Multi-Systems, Inc.	WinPM V1.62, V1.63, V1.80, V1.90	WinPM V1.95	
NCR	ScanMaster V1.1.6.xx All 1.2.xx.xx versions prior to V1.2.3.26 All 2.0.xx.xx versions prior to V2.00.03.12 All 2.1.xx.xx versions prior to V2.01.00.30	ACS V6.0 +	
	ACS V4.0	ACS V6.0 +	
Posera	Maitre'D All versions of V2002 All versions prior to V2003 service pack 11 All later versions prior to V2005 service pack 3	Maitre'D All later versions to and including V2003 service pack 11 All later versions to and including V2005 service pack 3	Maitre'D V2003 service pack 11 V2005 service pack 3
Radiant	Aloha All versions prior to V5.3.15	Aloha All versions later to and including V5.3.15	
Southern DataComm, Inc. (SDC) www.protobase.com	ConnectUp All versions	ProtoBase® V4.81.xx V4.83.xx	ProtoBase® Suite v6.00.xx
	PopsOn All versions	PbAdmin® V5.01.xx V5.02.xx	
	ProtoBase® V4.7x.xx V4.80.xx		
	PbAdmin® V4.01.xx V5.00.xx		



Payment Application Vendor	Product Version that May Retain Magnetic Stripe Data	Product Version/Patch that Does Not Retain Magnetic Stripe Data	PABP-Validated Product Version
VeriFone	Ruby, Topaz Buypack V2.08.xx, V2.09.xx, V2.10.xx, V4.01.xx	Ruby Buypack V4.08.xx	
	Ruby, Topaz (<i>Store & Forward Fleet and Debit</i>) Buypack V4.06.xx, V4.07.xx	Topaz Buypack V4.09.xx	

In addition to these payment applications listed above, there may be other applications that are currently storing prohibited data. Conversely, there also may be payment applications that do not store prohibited data that are not listed on Visa's list of validated payment applications. Visa encourages acquirers, VisaNet processors and third parties to notify Visa of other payment applications that may store prohibited data.

Recommended Mitigation Strategy

Agents and merchants are encouraged to utilize payment applications that have been validated against Visa's PABP available at www.visa.com/cisp. Agents and merchants using applications which store prohibited data should immediately upgrade to a version that does not retain prohibited data. This is accomplished by implementing an updated application version or patch made available by the vendor or 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. For VisaNet processors, Visa recommends that only PABP-validated payment applications be allowed to certify to the processor's payment platform. This requirement would greatly accelerate the security of the payment system and ensure all new payment applications are PABP-validated.

Often payment applications lead to the storage of prohibited data post-authorization without the merchant or agent's knowledge. Agents and merchants should ask all of their payment application vendors (or reseller / integrator) to confirm that software versions used do not store magnetic stripe data, CVV2, PINs or encrypted PIN blocks. This should be verified by asking the payment application vendor to share a list of files written by the application and a summary of the contents of those files. Agents and merchants must confirm that all cardholder data storage is necessary and appropriate for the transaction type.

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

Minimize Data Security Risks by Promoting Payment Applications Best Practices Validation

Visa recognizes the important role agents play within the payment system. As such, merchants depend on agents to provide them with secure ways to accept Visa payment cards. When driving merchants towards payment applications, agents should ensure the payment application has been validated against



Visa's PABP, available at www.visa.com/cisp. Visa is working toward making PABP an industry standard that is adopted by the Payment Card Industry Security Standards Council (PCI SSC).

Payment applications that do not adhere to PABP leave Visa members, agents, merchants and other stakeholders vulnerable to data compromises, and pose as an unacceptable risk to the entire payment system. Most importantly, payment applications utilized by agents and merchants must not store prohibited data, including full magnetic stripe data, CVV2 and PIN data following transaction authorization. If prohibited data is stored, corrective action must be taken immediately. Merchants and agents should be advised to use only payment applications that are included on Visa's list of PABP-validated payment applications.

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 validated against the PABP. To promote proactive compliance with the PABP, Visa is communicating directly with software vendors to help them better understand the value of PABP compliance and to encourage them to validate the conformance of their products to the PABP. Stakeholders are encouraged to refer to the list of more than 160 payment applications that have been validated against PABP, available on the Cardholder Information Security Program (CISP) Web site at www.visa.com/cisp.

Additionally, Visa will host three conference calls in August and September 2007 to review the information contained in this communication alert and to answer any questions from session participants.

Date: Monday August 27, 2007
Time: 8:00 – 8:30 AM PT
Dial In: 877-847-2001 ID: 00022067

Date: Friday August 31, 2007
Time: 9:00 – 9:30 AM PT
Dial In: 877-847-2001 ID: 00022067

Date: Monday September 10, 2007
Time: 8:00 – 9:00 AM PT
Dial In: 877-847-2001 ID: 00022067

If you cannot attend one of these calls and would like more information or have questions on this alert, please visit www.visa.com/cisp or contact cisp@visa.com.