Payment Processing Inc.

PPI MarketBulletin

Subject: PA-DSS Not Required for Secure Integration Methods (SIM)
Date: September 8, 2009

INTRODUCTION

Some payment gateway and payment software vendors are claiming that a Secure Integration Method (SIM) removes the need for PA-DSS compliance. This claim is counter to everything documented from the card brands and the PCI Security Council and creates a significant risk for software developers who accept the claim.

Extensive research indicates that:

- this SIM technology does not relieve software developers from the need to validate their applications
- it opens them up to potentially serious financial risk

PPI'S POSITION

Most providers of payment services and software are trying to limit, reduce, minimize or eliminate the cost burden for PA-DSS validation for software developers, but with importantly different methods:

- Some vendors are telling software developers “not to worry". They are stating that their wrapper integration removes compliance because it removes the storing, processing and transmitting card holder data.
- The PPI solution is to enhance software developer security by recognizing today’s PA-DSS requirements as simply a starting point and doing everything possible to protect our software partners and their customers.

PPI recognizes that ignoring the PCI Security Council's stance requiring wrappers like these to be certified is only part of the risk. The bigger risk is assuming that a certification alone makes you “secure”.

Remember, every major security recent breach has happened to organizations that were certified.

Our Partners have three choices:

1) Trust that vendors claiming "no need for compliance" are correct in the face of documentation that contradicts their position.

2) Get certified...and hope that is enough.
3) Actively become secure with a partner than can reduce the cost of validation and provide security beyond PCI.
    a. This is PPI's position, and we will work with our partners to minimize the cost burden....probably eliminate it....and hopefully, in time, take the partner out of scope altogether by obtaining approval from the PCI Security Council.

WHO MAKES THE RULES?

The PCI Security Council is the exclusive governing body that determines compliance standards.

https://www.pcisecuritystandards.org/

- The PCI Security Standards Council is an open global forum for the ongoing development, enhancement, storage, dissemination and implementation of security standards for account data protection.

- The organization was founded by American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa, Inc.
- PCI DSS follows common sense steps that mirror best security practices.
- The DSS globally applies to all entities that store, process or transmit cardholder data.

PCI SECURITY COUNCIL'S RULING ON: "WRAPPER" TECHNOLOGY ELIMINATION PA-DSS VALIDATION REQUIREMENTS

PCI SECURITY COUNCIL OFFICIAL COMMUNICATION
CASE REFERENCE NUMBER: Ref#: 0402093017
DATE: April 2, 2009

QUESTION

I am the Director of Developer Services in charge of the Integration and PCI Compliancy groups at Payment Processing, Inc. We are a processor that has our own gateway called PPI PayMover that is a hosted solution that our partners integrate to.

We are researching the idea of being able to provide a "PCI Proof" module for both our gateway and 3rd party products. I am sure you are aware that there are providers that claim that if you, the POS provider integrate our solution, you will not need to go through PA-DSS because it will encapsulate all of the transaction data from you so that you never see it and are not storing, processing or transmitting the credit card data itself. Does the PCI SSC agree that it is possible

to have a product that POS providers can integrate to without going through PA-DSS themselves?

If you could provide an opinion on how the PCI SSC stands on this or any research or actions that are currently being taken, we would be very grateful. This is very much a gray area for us that we would like some clarity on.

ANSWER
From: PCI Info [mailto:info@pcisecuritystandards.org]
Sent: Thursday, April 02, 2009 1:31 PM
To: Dave McMath
Subject: Reply to your question for PCI SSC RE: POS Providers (Ref#: 0402093017)

Dear Mr. McMath,

Thank you for your interest in The PCI Security Standards Council.

The *answer to your inquiry is as follows. Your original query follows below:*

The product the POS providers integrate to that encapsulates the transaction data (a "wrapper" here) may elect to go through a PA-DSS review since it is a third-party payment application that is part of authorization or settlement, and the POS products that integrate to it would also be included in the wrapper's PA-DSS review. The wrapper's PA-DSS review alone would not exempt a POS application since the POS and the wrapper would need to be reviewed together to ensure that all functionality works.

Thank you and regards,

The PCI Security Standards Council Response Team

info@pcisecuritystandards.org

781-876-8855

ARE THERE ANY OTHER VENDORS THAT OFFER A "WRAPPER" INTEGRATION THAT REQUIRE PA-DSS VALIDATION?

Verifone, a reputable payments solution company that generated $201 million in revenue in three months ending 4/30/09, offers a wrapper integration with their PAYware PC payment software package. PAYware SIM Version 2.0.0 was PA-DSS certified on 5/20/09.

Verifone has clearly stated in a press released 4/21/09 that PA-DSS validation using this product is needed and has provided a reduced cost validation services with a QSA (qualified security assessor).

LAS VEGAS - April 21, 2009 – (ETA Booth #219) – VeriFone Holdings, Inc. (NYSE: PAY), today announced PAYware SIM, providing a single interface to simply and securely integrate Windows-based POS systems with VeriFone's secure payment software solutions and consumer activated acceptance devices. The developer tool isolates sensitive cardholder data from the POS application, and is designed to greatly reduce the complexity and associated costs of achieving compliance with PCI and PA DSS requirements.

http://www.verifone.com/2009/payware-sim-to-securely-integrate-payment-devices.aspx

WHAT WILL HAPPEN TO PARTNER CUSTOMERS IF THEY ARE NOT COMPLIANT?

FINES

If there is a breach the partner's customer can expect fines, forensic charges and card replacement costs. Visa states the following on their web site regarding fines for customers that are not compliant:

COMPLIANCE FINES

If a member, merchant or service provider ***does not comply*** with the security requirements or fails to rectify a security issue, ***Visa may fine the responsible membe***r. ***Visa may waive fines*** in the event of a data compromise if there is no evidence of non-compliance with PCI DSS and Visa rules. ***To prevent fines*** a member, merchant, or service provider must maintain full compliance at all times, including at the time of breach as demonstrated during a forensic investigation. Additionally, a member must demonstrate that prior to the compromise the compromised entity had already met the compliance validation requirements, demonstrating full compliance.

Source: http://usa.visa.com/merchants/risk_management/cisp_overview.html

IMPACT ON BEING ABLE TO PROCESS

Visa has already issued mandates relating to the use of non-compliant applications. They can be found on the Visa site:

http://usa.visa.com/merchants/risk_management/cisp_payment_applications.html

These mandates are directed to the partner's customers. The mandates will impact the boarding of new customers and continued ability to processing transactions. Each processor will determine the processes for validation of these mandates. Processors will deny new customers and/or require that customers using non-compliant applications cease processing payments.

Processors are already implementing these mandates and the implementations will likely change as new mandate dates pass.

HOW WILL THIS IMPACT OUR PARTNERS?

We believe that there are three significant ways a partner's revenue could be negatively impacted by not being compliant:

1) If a non-compliant customer is breached and is using a non-compliant software application, then the customer will likely incur fines and the fines will be a result of the software application. This will no doubt impact our partner's ability to be competitive and sell new systems.

2) When the processors require validation of PA-DSS, it is likely that a non-validated partner could sell a new system and the customer will not be able to get a merchant account.

3) In addition, if a partner has a non-validated application, the processor could remove processing abilities for every customer using that partner's application.

These are serious risks for our partners that could have catastrophic impacts on their business. As a payment partner it is PPI's responsibility to protect our partners and their customers.

INVESTIGATE

For software developers, this is an issue that could impact their business in a significantly negative way. PPI recommends that software developers investigate the claims by taking action on the following:

1. Is there proof from the PCI Security Standards Council?
    a. Ask for the validation letter from the PCI Security Council.
    b. The QSA letter is not the official acceptance of the validation.
2. Email the PCI Security Standard Council concerning reference # 0402093017.
    a. Phone 781-876-8855
    b. FAQ - submit a question
        i. http://selfservice.talisma.com/display/2/_index1.aspx?tab=atr&r=0.1930701
3. Is the "hosted pages - web forms" function listed on the Visa approved PCI DSS services listing?
    a. http://usa.visa.com/merchants/risk_management/cisp_service_providers.html
4. Is the partner a member of the PCI Security Standards Council?
    a. https://www.pcisecuritystandards.org/participation/member_list.html
5. Ask PPI about the PA-DSS scope relief program.

SUMMARY

There are many details and many unknowns but the risks for our partners are real and large. The issue comes down to one simple question; "Is a SIM implementation going to relieve the burden of validation from software developers?"

Today this type of integration is in scope. There is no evidence that the PCI Security Council or the card brands will ever release the burden of validating software applications. There is no doubt that as a partner we must do everything possible to reduce the financial burden of validation from our partners and we have done that.

Because of the enormity of the risk we believe that our partners should "Get on the List" and they should be able to do it at a reasonable price if not for free.