

Payment Card Security

By

Don West, CPA, CISA, CISSP, PMP, CITP

Blytheco, LLC

Albert Gonzalez and two others were charged in August with hacking into the computer systems of Heartland Payment Systems, 7-Eleven and Hannaford Brothers and stealing data on over 130 million credit and debit cards. Gonzalez was already in jail on charges that he had hacked TJX (T.J. Maxx, Marshalls and more). That case involves 47.5 million cards. In each case the intrusions went on for months before being detected.

If an organization stores, processes or transmits payment card Primary Account Numbers (PAN) it must comply with the industry requirements for data security. Compliance doesn't guarantee security but it helps. Not complying can result in fines, adverse publicity and loss of the ability to accept payment cards.

Compliance is difficult and expensive even for larger merchants. It can be prohibitive for smaller ones. You can greatly reduce the cost and effort by reducing your exposure, by not storing cardholder data electronically.

PCI (Payment Card Industry) Security Standards Council

The payment card industry has been working for years to increase the security of card data. At first the card associations established their own policies and standards. In 2006 Visa Inc., MasterCard Worldwide, American Express, Discover Financial Services and JCB International formed the PCI Security Standards Council and agreed to incorporate the resulting standards and certifications into their compliance programs.

PCI Data Security Standard (DSS)

The foundation of the Councils work is the Data Security Standard. Version 1.2.1 was released in July, 2009. It is a very specific and detailed list of requirements for securing card holder data. It contains hundreds of requirements organized as follow:

Build and Maintain a Secure Network

Requirement 1: Install and maintain a firewall configuration to protect cardholder data

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

Protect Cardholder Data

Requirement 3: Protect stored cardholder data

Requirement 4: Encrypt transmission of cardholder data across open, public networks

Maintain a Vulnerability Management Program

Requirement 5: Use and regularly update anti-virus software or programs

Requirement 6: Develop and maintain secure systems and applications

Implement Strong Access Control Measures

Requirement 7: Restrict access to cardholder data by business need to know

Requirement 8: Assign a unique ID to each person with computer access.

© Copyright 2009



Requirement 9: Restrict physical access to cardholder data.
Regularly Monitor and Test Networks
Requirement 10: Track and monitor all access to network resources and cardholder data.
Requirement 11: Regularly test security systems and processes.
Maintain an Information Security Policy
Requirement 12: Maintain a policy that addresses information security for employees and contractors.

PCI Payment Application Data Security Standard (PA-DSS)

This standard started as the Visa Inc. program known as the Payment Application Best Practices. Its goal is to help software vendors and others develop secure payment applications that support compliance with the PCI DSS.

Qualified Security Assessors (QSAs), Payment Application QSAs (PA-QSAs) and Approved Scanning Vendors (ASVs)

QSAs, PA-QSAs and ASVs are companies and individuals certified by the Council to perform required services for the higher level merchants (See the table below).

Applicability

Applicability of the standards to a particular entity can be confusing. The main rule is:

“PCI DSS requirements are applicable if a Primary Account Number (PAN) is stored, processed, or transmitted. If a PAN is not stored, processed, or transmitted, PCI DSS requirements do not apply.”

Generally the deadlines for compliance with the DSS have passed and all merchants who meet this rule should be compliant now. Estimates of actual compliance vary.

The issuing associations direct the acquiring banks as to how they manage merchant compliance. An example is merchant levels based on card acceptance volume. The following table shows the Visa levels and validation requirements.

Level / Tier	Merchant Criteria	Validation Requirements
1	Merchants processing over 6 million Visa transactions annually (all channels) or Global merchants identified as Level 1 by any Visa region ²	Annual Report on Compliance ("ROC") by Qualified Security Assessor ("QSA")
		Quarterly network scan by Approved Scan Vendor ("ASV")
		Attestation of Compliance Form
2	Merchants processing 1 million to 6 million Visa transactions annually (all channels)	Annual Self-Assessment Questionnaire ("SAQ")
		Quarterly network scan by ASV
		Attestation of Compliance Form
3	Merchants processing 20,000 to 1 million Visa e-commerce transactions annually	Annual SAQ
		Quarterly network scan by ASV
		Attestation of Compliance Form
4	Merchants processing less than 20,000 Visa e-commerce transactions annually and all other merchants processing up to 1 million Visa transactions annually	Annual SAQ recommended
		Quarterly network scan by ASV if applicable
		Compliance validation requirements set by acquirer

Notice that Level 1 merchants, those with the highest volume, are required to employ QSAs and ASVs and submit reports. Level 4 merchant validation requirements on the other hand are either recommended or set by their acquiring bank.

Each card association sets its own levels and validation requirements. American Express for example only has three levels. The rule of thumb is that each merchant should consult their acquiring bank.

Requirements also vary greatly depending on how you handle cardholder data (CHD).

Self-Assessment Questionnaire (SAQ)

The Self Assessment Questionnaire referred to in the table above is actually four different questionnaires depending on how CHD is handled. The following table shows the SAQ Validation Types.

SAQ Validation Type	Description	SAQ: V1.2
1	Card-not-present (e-commerce or mail/telephone-order) merchants, all cardholder data functions outsourced. This would never apply to face-to-face merchants.	<u>A</u>
2	Imprint-only merchants with no electronic cardholder data storage	<u>B</u>
3	Stand-alone terminal merchants, no electronic cardholder data storage	<u>B</u>
4	Merchants with POS systems connected to the Internet, no electronic cardholder data storage	<u>C</u>
5	All other merchants (not included in Types 1-4 above) and all service providers defined by a payment brand as eligible to complete an SAQ.	<u>D</u>

Type 1 merchants outsource everything and never have CHD in their systems. SAQ A has 13 questions. Types 2 and 3 either use paper only or the small terminals that are not connected to the Internet or internal systems and do not store CHD electronically. SAQ B has 26 questions. Type 4 merchants use a Point of Sale (POS) system connected to the Internet but no internal systems. They do not store CHD electronically. SAQ C has 41 questions.

Validation Type 5 merchants store CHD electronically and must answer 225 questions. Obviously the key is to not store CHD electronically.

Note: Service providers are entities that process CHD for merchants. They are outside of the scope of this article.

Onerous requirements for small merchants

The requirements of the DSS for merchants that store CHD electronically are extremely complex and expensive. Here are a few examples:

1. DSS 1.3 requires segregating the CHD network from the Internet and passing all inbound and outbound traffic through a Demilitarized Zone (DMZ). This means additional hardware, configuration and management.
2. DSS 10.5.5 requires file integrity monitoring. This means adding systems that constantly monitor critical files within the CHD system, operating system files for instance, and notify you of any changes. More hardware, software and management.

3. DSS 10.6 requires that log files for all components in the CHD system are kept for months and reviewed daily. This can be thousands of entries per day. More hardware, software and management.

This is a small sample of the requirements. As I said earlier, meeting these requirements is very difficult and expensive.

Alternatives for small merchants

Large merchants can justify implementing and maintaining compliant systems. Many smaller, Level 4, merchants can't. The answer is to not store CHD electronically. In other words, don't be a SAQ D merchant.

If you accept cards on line there are two basic ways to do it. I'll use PayPal as an example. PayPal offers "PayFlow Pro" and "PayFlow Link" as ways that a web site can accept payment cards.

With PayFlow Pro, buyers enter their card data on your web site. Your system sends the card data to PayPal for processing and PayPal sends the results of the transaction back to your system. Your system stores CHD electronically and you are a SAQ D merchant.

If you use PayFlow Link, when the buyer is ready to check out he or she is sent to a PayPal web page. All card data is entered in PayPal's system, not yours. Your system still receives transaction results but it does not store CHD electronically. You are now a SAQ A merchant.

If you are a face-to-face merchant, a retail store or restaurant for example, it can be more complicated. If your Point of Sale (POS) system does not store CHD electronically you are a SAQ C merchant. As I said above, SAQ C only has 41 questions and answering them satisfactorily is much easier than those on SAQ D. If your system stores CHD electronically, as a great number of them do, you are a SAQ D merchant.

So the question is, do you need to store CHD electronically? There are several reasons to do so. One is as a service to the buyer to make it easier to make a purchase on your web site. Amazon's "One Click Ordering" is an example. It is automatically enabled on your account the first time you place an order and enter your information. Some people love it. It can't work without storing your CHD electronically. Even without the one click service a lot of sites store your data just to make it easier for you to make a purchase.

If you go into a sports bar and order a drink you may be asked for a card before you are served. Some just put them in a box and hold them. (The wisdom of that and you allowing it is outside the scope of this article) Some pre-approve some amount on the card. That POS system is storing your CHD. They do it to prevent you from walking out without paying.

A very popular reason to store CHD is to handle charge backs. Frequently people will make a purchase and then claim they didn't do it. Many merchants think they have to have the card data to prove it was a valid purchase. This is not true and even if it was the merchant would have to compare the cost of charge backs to the cost of PCI compliance. After telling a small merchant that compliance would cost him tens of thousands of dollars he said he had to have the CHD to fight charge backs. I asked him how many he had, and he said a couple per month. His average charges are under \$100.


Conclusion

Payment card data security is a huge concern and will get worse before it gets better. All organizations that store, process or transmit Cardholder Data must comply with the PCI DSS. Compliance is either relatively painless or an expensive, demanding, ongoing process depending on how you accept and process cards.

Breaking News!

I mentioned earlier that Level 4 validation requirements were set by the acquiring banks. Until recently this has remained mostly a voluntary process of self assessment with no requirement to submit the forms to anyone. On August 1 BB&T notified all of its merchant account holders that they had to complete and submit the self assessment forms, including an Attestation of Compliance by the Executive Officer. First National Merchant Services and First American Payment Systems have done the same thing.

Voluntary self assessment for the smallest merchants is quickly becoming a thing of the past.



Blytheco LLC The Premier Provider of Effective Business Software Solutions

**National Presence
Local Touch**

Sage Software Business Partner of the Year

Regional Headquarters

Orange County, California 23161 Mill Creek Drive, Ste. 200 Laguna Hills, California 92653 Phone: (949) 583.9500 Toll Free: (800) 425.9843 Fax: (949) 583.0649	Atlanta, Georgia 1100 Johnson Ferry Road, Ste. 450 Atlanta, Georgia 30342 Phone: (404) 841.6240 Toll Free: (800) 455.1368 Fax: (404) 841.6243
---	---

www.blytheco.com **solutions@blytheco.com**

Complete Sage Software Solutions
Sage MAS 500 ◦ Sage MAS 200 ◦ Sage MAS 90
Sage BusinessWorks ◦ Sage SalesLogix CRM ◦ ACT! by Sage
Sage ABRA HRMS ◦ Sage FAS ◦ Sage MIP Fund Accounting & Fundraising

Offices in these cities:
ATLANTA GA COLUMBIA SC COLUMBUS OH DALLAS TX DENVER CO
GREENVILLE SC LOS ANGELES CA MINNEAPOLIS MN ORANGE COUNTY CA TAMPA FL