

Any merchant that accepts credit cards for payment (e.g., restaurants, retail stores, service providers) will be expected, if not required, to be PCI compliant. The Payment Card Industry Data Security Standard (PCI DSS) was developed in late 2004 by the major credit card companies following the increased frequency of data breaches. The credit card companies had to find a way to hold merchants responsible for data breaches since companies like Mastercard, Visa, American Express, Discover and the issuing banks were incurring major expenses after a breach. They have had to change card numbers, absorb fraudulent charges, pay for the issuance of new credit cards and incur other expenses. The standards have been revised multiple times since 2004. (See the following page for a summary of the current standards.)

Not only are there data security requirements, but there are fines for non-compliance with the PCI standards. These fines can be hundreds of thousands of dollars and are often levied against the merchant without any formal proceeding to negotiate the fine. This article has a nice summary of the issue:

<http://www.restaurant.org/profitability/datasecurity/briefing/index.cfm>.

Here's an excerpt from the article of particular concern:

Merchants' transaction-processing agreements with banks usually require merchants to comply with card-network operating rules. They can also require merchants to be financially responsible for damages and penalties assessed by card networks for PCI violations. **In many cases, the fines and damages automatically are deducted from money owed to merchants for completed transactions.**

We know that just about every Cyberliability form has fines and penalties excluded in their definition of loss with the exception of regulatory fines and penalties. The PCI fines are contractually driven and are often additionally excluded by breach of contract exclusions and specific Merchant Agreement exclusions. A few markets have started providing small sublimits of coverage for these fines.

A small sublimit can be somewhat helpful, but what if you have a very large fine, which is withheld from the merchant by the payment card processor? A sublimit covering a portion of a fine after it is levied is clearly not good enough. The merchant will want to prevent or reduce that fine before funds are withheld. It is easier to negotiate a fine before a decision is made than fight to overturn a fine. There are now some attorneys specializing in fighting the fines, but they are not working for free.

What's the AmWINS solution to this? In conjunction with one of the leading providers of Cyberliability insurance, we have created an endorsement to provide assistance for this troubling problem. Our insurer will provide up to \$50,000 for the cost of an attorney to prepare for the administrative process required by a Merchant Services Agreement in connection with a security breach. The attorney will assist the insured to collect information, complete the administrative procedure required under the Merchant Services Agreement, and work on a compromise or reduce the amount of any damages or fines assessed against the insured. Our insurer requires the use of their recommended attorney. *There is currently nothing else like this in the market.*

Please contact your AmWINS Financial Service Broker to make sure your clients are getting this innovative coverage enhancement.

To learn more about how AmWINS can help you place cyberliability coverage, reach out to your local AmWINS broker or marketing@amwins.com.

If you do not have a contact at AmWINS to help with your financial services risks, [click here for a list of brokers on our website](#).

Legal Disclaimer: Views expressed here do not constitute legal advice. The information contained herein is for general guidance of matter only and not for the purpose of providing legal advice. Discussion of insurance policy language is descriptive only. Every policy has different policy language. Coverage afforded under any insurance policy issued is subject to individual policy terms and conditions. Please refer to your policy for the actual language.

 AmWINS
Group, Inc.

AmWINS Group, Inc. is a leading wholesale distributor of specialty insurance products and services. AmWINS has expertise across a diversified mix of property, casualty and group benefits products. AmWINS also offers value-added services to support some of these products, including product development, underwriting, premium and claims administration and actuarial services. With over 1,800 employees located in 16 countries, AmWINS handles over \$5 billion in premium annually through our four divisions: Brokerage, Underwriting, Group Benefits and International.

CLIENT ADVISORY

Unique New PCI Endorsement Helps Address Challenging Cyberliability Issue

The PCI Data Security Standard

PCI DSS is the global data security standard adopted by the payment card brands for all entities that process, store or transmit cardholder data. It consists of common sense steps that mirror security best practices.

GOALS	PCI DSS REQUIREMENTS
Build and Maintain a Secure Network	<ul style="list-style-type: none"> Install and maintain a firewall configuration to protect cardholder 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 cardholder data. Encrypt transmission of cardholder data across open, public networks.
Maintain a Vulnerability Management Program	<ul style="list-style-type: none"> Use and regularly update anti-virus software or programs. Develop and maintain secure systems and applications.
Implement Strong Access Control Measures	<ul style="list-style-type: none"> Restrict access to cardholder 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 for all personnel.

Source: <https://www.pcisecuritystandards.org/documents/PCI%20SSC%20Quick%20Reference%20Guide.pdf>