

A hand in a white sleeve holds a scale against a background of a city skyline at night. The scale is tilted, and the text 'GOT COMPLIANCE?' is written across it in large, red, 3D letters. The hand is positioned at the top, with the scale's ropes hanging down. The city skyline is visible at the bottom, with lights and buildings. The overall tone is dramatic and emphasizes the weight of compliance.

**GOT
COMPLIANCE?**

**TURN PCI COMPLIANCE
MANDATES INTO CUSTOMER
SERVICE OPPORTUNITIES**

by Dana Poynter

As cases of consumer fraud, identify theft and security breaches continue to make the news, the Payment Card Industry (PCI) is progressing toward insuring security for cardholder data. And, while most merchants work to meet mandated certification and validation of their systems, the technological nightmare and financial havoc of non-compliance continues to rear its ugly head.

As an ISO, you may wonder what that means to you. The fallout of non-compliance has a domino effect on your business, as the financial implications of a breach can destroy merchants of any size. When a business ceases to operate, so does its related income stream, and that hurts your bottom line. Continued losses due to compliance can even put your reputation at risk. You can avoid that black hole altogether by exceeding the validation requirements for signing on new merchants or continuing service for existing ones. Utilize PCI compliance as an opportunity to deliver on the promise of excellent customer service, and add a PCI security requirements educational component to your communication list of to-dos with merchants.

Who better to educate merchants about PCI standards than the people who supply them with credit card payment and processing capabilities? In fact, many merchants are coming to expect that kind of education from their merchant services providers. Many ISOs have already

started educational programs that bank on the real opportunity to organically grow business. They are providing industry knowledge and information that small merchants need. Turning PCI compliance into an educational opportunity for merchants is helping these ISOs deliver excellent customer service that keeps their merchants "in-the-know" about the latest updates and requirements.

Take Stock

Now is the time to take stock of the challenges PCI compliance poses to your merchants and educate them about DSS standards and implementation. Everyone has a general understanding of PCI – compliance that is required of all merchants and any entity that stores, transmits or processes cardholder data. A framework for safeguarding sensitive data for all credit card brands, the program applies to all acceptance environments, including retail (bricks-and-mortar), mail-or telephone-order and e-commerce.

A few questions can help you take stock of each merchant's understanding of, and commitment to, compliance on a basic level. The first three questions are essential components in a PCI compliant environment and, when not up-to-date, account for the greatest opportunity for compromise.

- Is virus protection up-to-date and provided by a reputable company?

- Are the latest software revisions, such as security patches, in place for the operating system?

- Is adequate firewall protection installed and up-to-date?

- What vendor provides payment software? Has software been created internally? Does the payment application store card numbers, track data or PIN data?

- How many people have access to cardholder data?

- Are passwords changed frequently, and do they differ from default passwords?

- Are back office procedures compliant – procedures such as storing paper reports under lock and key and limiting personnel access?

- Where is sensitive data stored? How many people can access it?

- Are mobile computing devices, such as laptops, PDA's and those with wireless access also PCI compliant?

Getting there is half the battle. In order to move beyond a basic understanding and grasp the financial implications of non-compliance, merchants need a greater awareness of how costly a breach can be to both their operational reputation and bottom line. Fear can be a great motivator, but it also detracts from merchants' interest in facing the compliance battle head-on. Herein lies the educational communication opportunity and value that ISOs can deliver:

Communicate Value

Communicating the value of PCI compliance can be hard to do without playing into the fear that system upgrades underscore big spending. For many smaller merchants, that is a valid concern, but one that is quieted by the harsh and expensive reality of non-compliance. Unfortunately, there is no easy cost comparison available, as the expense of upgrades relies on many factors: existing infrastructure, hardware, software, security features, back office processes and encryption methods to name a few. Fewer of these in place translates to higher front-end expenses. But, to continue business as usual, these upgrades are a necessary evil to avoid potentially hundreds of thousands of dollars in fines and technological assessments.

Communicate Cost

- ▲ Provide an overview of anticipated costs associated with non-compliance:
- ▲ Damage to brand/reputation
- ▲ Investigation and remediation costs
- ▲ Ongoing compliance audits
- ▲ Victim notification costs
- ▲ Financial loss
- ▲ Fines and fees from each card brand for noncompliance, reissuance, fraud loss and ADCR
- ▲ Data loss
- ▲ Chargebacks for fraudulent transactions
- ▲ Operations disruption
- ▲ Sensitive information disclosure
- ▲ Denial of service to customers
- ▲ Possibility of business closure
- ▲ Potential legal liabilities beyond the Association rules

Communicate Simplicity

Once system-wide security standards are met, merchants may be confused about the rules and regulations to verify compliance. They may even be concerned that there are too many hoops to jump through. Since non-compliance is non-negotiable, break the process down into a simple to-do list and help merchants understand their responsibilities.

Level 1 merchants must provide an Annual on-site assessment by a Qualified Security Assessor or internal audit if signed by an officer, as well as Quarterly Network Scans by an Approved Scanning Vendor.

Level 2 and 3 merchants need proof of compliance including certification of an Annual self-assessment questionnaire and Quarterly network security scans performed by an Approved Scanning Vendor.

Level 4 merchants are not currently required to provide certification or verification, although it is recommended. As an ISO, you may find it increasingly difficult to sign-on new merchants who cannot provide proof of compliance.

Communicate Resources

Merchants may need assistance with upgrading systems, understanding the verification process, analyzing security risks, comprehending the cost of non-compliance or evaluating their overall needs. Communicate with them about valuable resources and trusted, qualified vendors that can provide the kind of assistance they need. For every PCI requirement, there are specialists who can make the process much smoother.

As well, check with your own acquirer to find out what kind of services and information they offer to your merchants with regard to PCI, such as free risk assessments and connection to qualified vendor relationships in the security and assessment industries. Use that information as a gateway to the discussion and once the door is open, help them understand what is involved with annual assessments and quarterly verifications and how to stay up-to-date with standards and regulations.

Ultimately, PCI compliance is the best form of insurance against the kind of breaches that can cost businesses everything and destroy future business opportunities.

If you don't educate your merchants about compliance, who will? Utilize your knowledge to position yourself as an expert in the delivery of strong customer service that merchants rely on. You have an opportunity to provide exemplary service to your merchants, and protect and grow your own business by establishing an ethical, educated reputation that other merchants will seek.

For More Information

Please refer to www.pcisecuritystandards.org for a complete review and printable version of the current PCI standards that describe the 12 PCI DSS requirements. ■

Dana Poynter oversees merchant compliance as the Vice President of Global Compliance at Elavon (formerly NOVA Information Systems). She is regarded as a PCI Compliance expert in the field, having been in the payments industry for almost twenty years.