

# Are You In Compliance? Credit Card Security Matters

By Ericka Schwarm



**For the past few years, the same news story has garnered headlines over and over again. A retailer, restaurant chain or lodging provider was the victim of a credit card hack. As I write this, it was just revealed that Whole Foods and Sonic are the most recent to experience a breach of customer credit card data.**

If you want to protect your

customers—and your company's reputation—from a similar fate, there's one term you need to learn and pay attention to right away: PCI DSS compliant.

What does it mean? The Payment Card Industry Data Security Standard is an information security standard for organizations that handle branded credit cards from the major card

companies. Launched more than a decade ago, the PCI Security Standard Council (PCI SSC) is an independent body created by some major card brands (Visa, MasterCard, American Express, Discover and JCB) to manage the ever-changing payment landscape and ensure that the most up-to-date security measures are in place to protect cardholders. The standards are in place to ensure that

companies maintain a certain security standard in their practice of accepting, processing, storing or transmitting credit card information. Validation of compliance is performed annually, either by an external Qualified Security Assessor (QSA) or by a firm specific Internal Security Assessor that creates a report on compliance for organizations handling large volumes of transactions, or by Self-Assessment Questionnaire (SAQ) for companies handling smaller volumes.

The assessments measure compliance with the standards that any organization that accepts, stores or transmits cardholder data are held to. Cardholder data is defined by the PCI SSC as “the full primary account number (PAN) or the full PAN along with either the cardholder name, expiration date or service code.” There are four levels that merchants fall under, which are based on the volume of transactions processed. However, certain risk factors can put a merchant into a higher level based upon the card issuer’s determination.

There are penalties for non-compliance, which vary between the payment brands. According to PCI Compliance Guide, they may, at their discretion, fine an acquiring bank \$5,000 to \$100,000 per month for PCI compliance violations.

**If you want to protect your customers—and your company’s reputation—from a similar fate, there’s one term you need to learn and pay attention to right away: PCI DSS compliant.**

Usually, the bank will pass this fine over to the merchant, and will often either terminate the bank/merchant relationship or increase transaction fees. Hefty fines and being labelled as high-risk can spell big trouble for many



small businesses. By establishing top-tier security practices from the start, you can potentially save your business a significant amount of financial burden in the future.

According to Verizon’s 2017 Payment Security Report, only 55.4 percent of companies meet all PCI DSS compliance standards. While this

number is up 7 percent from 2015, it still translates to nearly half of retailers, IT services companies, payment software providers and hospitality organizations do not adequately protect credit cardholder information.

Additionally, 44.6 percent of companies fall out of PCI DSS compliance within nine months of validation.

The report listed results for the hospitality sector separately. Less than half (42.9 percent) of hospitality organizations achieved full compliance at interim assessment in 2016—the lowest of the four key verticals. Only a quarter (25.0 percent) of hospitality organizations in the Americas achieved full compliance at interim assessment.

When choosing a credit card processor, it’s imperative that you select one that has achieved and maintained PCI compliance. I’m proud to say that Equiant has made this a priority. We recently again received the Payment Card Industry Security Standards Council’s highest level of certification: PCI Certification Level 1. The PCI Level 1 certification provides yet another reassurance that Equiant can accept, process, store and transmit



Ericka Schwarm recently joined the Equiant Financial Services team as the Director of Client Development where she plays a critical role being a Proactive Client Advocate and Business Matter Expert. She focuses on continuous improvement initiatives and trainings, and coordinates the business relationships between the Client and Equiant. Her career in the Vacation Ownership Industry began in 2011 when she joined The Conrad Companies as the Director of Sales and Marketing. Prior to joining Conrad, she was Assistant Vice President and Vice President at two major financial institutions in the Retail Consumer Banking divisions. With this experience, Ericka brings significant financing and relationship management knowledge.

Ericka graduated from Northern Arizona University with a Bachelor of Arts in International Affairs with a concentration in Business Economics and is currently working on her Registered Resort Professional (RRP) designation through ARDA.

**Ericka Schwarm**  
**Director of Client Development**  
**p 480.636.4892 | m 480.737.0389**  
**eschwarm@equiant.com**

credit card information on client's behalf in a secure environment. Equiant has maintained its PCI Level 1 Certification since it first applied in 2011 and remains the only loan servicing company serving vacation ownership developers to receive the coveted certification. Equiant is also a member of the prestigious Visa Global Registry of Service Providers ([www.visa.com/splisting](http://www.visa.com/splisting)), demonstrating its commitment to strict security standards and full compliance with PCI regulations. As Visa recommends, "Clients and merchants should reference the site regularly as part of their due-diligence process and should only use service providers that are listed on the Registry for outsourcing their payment-related services."

If your business accepts credit card payments, you need to be concerned about it, too. In addition to the penalties for non-compliance, there

on your app? Will they be willing to allow your app to access their contacts and other personal information?

Here's where that PCI DSS compliance proves its worth. According to the Verizon reported mentioned above, of all the payment card data breaches that Verizon has investigated between 2010 and 2016—nearly 300—not a single organization was fully PCI DSS compliant at the time of the breach.

It goes without saying that protecting your organization and your owners' and members' personal data from outside threats is of ultimate importance to you. Making sure that you're in the know on PCI compliance is an important step in making sure that protection is in place.

Ericka Schwarm is director of client development at Equiant, one of the leading timeshare servicers in the United

**According to PCI Compliance Guide, they may, at their discretion, fine an acquiring bank \$5,000 to \$100,000 per month for PCI compliance violations.**

are other sound, common-sense, self-interested reasons to comply voluntarily.

As we move further into the digital age where we are asking consumers to download our apps and share more and more personal information with us, it's even more important to prevent a data breach.

In a recent consumer survey, 66 percent say they would be unlikely to do business with an organization that experienced a breach where their financial and sensitive information was stolen. And even if they would trust your company with a credit card transaction again, would they be willing to share their location with you

States with a portfolio that exceeds \$1 billion and includes more than 125,000 individual consumer loans. Over the past 28 years, Equiant has serviced more than 1.5 million loans and 1.25 million maintenance fees accounts. Its array of products and services includes loan receivables and maintenance fee servicing on a fully hosted web platform, Platform as a Service (PaaS) receivables technology, point of sale merchant processing, delinquency control, document custody (including digital), and analytic reporting. To learn more about Equiant's industry-leading security and receivables servicing, call Schwarm at (480) 636-4892 or Peter Moody, vice president of business development, at (480) 636-4888 or visit [www.equiant.com](http://www.equiant.com).