# PCI DSS Compliance across Retail and Financial Services

## PCI DSS Complexities

With its requirements in place for well over a decade, the Payment Card Industry Data Security Standard (PCI DSS) has effected many changes across the retail and financial services industries. This industry regulation's stringent yet prescriptive security requirements have improved information security programs, built out IT resiliency, and minimized overall business risks in countless ways across businesses of all sizes. PCI DSS has set the standard and changed the way that many organizations approach security, compliance, and overall IT governance. Based on my observations and experience working in these industries along with what the security studies are showing, PCI DSS is having a lasting impact.

Of all the compliance regulations I have consulted with clients on with over the years (HIPAA, GLBA, etc.), PCI DSS is the one that stands out. Why is that? Is it related to the high-risk, and thus high-security, nature of financial services? Perhaps it's because of the high-profile retail security breaches we've seen in recent years? Maybe it's because of the severe penalties associated with noncompliance or the fact that it's an industry—rather than government—regulation. I'm not fully sure but I do know that PCI DSS addresses security from all the right angles, including authentication and access control, patching, and specific requirements around ongoing vulnerability and penetration testing. I think part of what has helped businesses establish and maintain buy-in on PCI DSS is its level of specificity on what needs to be done.


Still, PCI DSS compliance doesn't mean security perfection. Retail and financial services incidents and breaches still occur.

The interesting thing about PCI DSS compliance is that given all of the efforts involved, i.e., QSA audits, ASV vulnerability scans, and those who have to complete the self-assessment questionnaires, an organization can be fully compliant with PCI DSS right up until the point of a breach. Documentation is in place, processes appear to be working, and technical controls are implemented—yet the unthinkable occurs. Somewhere, somehow along the way someone forgot to do something correctly. Or, perhaps, technical controls were what I like to call under implemented—a situation where the controls are in place but not being utilized as intended or to their fullest potential. There could even be situations such as weaknesses in business

### Top PCI DSS Facts to Keep in Mind

1. Validation of compliance is not a check off item. It requires annual third party and internal assessments
2. If your organization is hacked or found to be breaching PCI regulations, you may face hefty fines
3. There are four levels of compliance
4. If you experience a data breach you then must meet the most stringent merchant assessment criteria (not at all pleasant or cheap)

processes or core systems were never uncovered and people with ill intent found and exploited them.

## Sources of Risk

Looking at the bigger picture, there are some areas of risk and, thus, opportunity that need to be addressed in the context of PCI DSS compliance. Regardless of your level of security maturity, you need to pay special attention and continually look for gaps involving cardholder data access. That's what it really boils down to. Many people search for the latest techniques or advanced technologies to help solve this challenge but it's just not necessary in most environments. Instead, it's just taking the core principles associated with access control and doing them really well.

Reduction in PCI scope is a key part of maximizing access control. I still see a lot of systems that store and process cardholder data outside the perceived cardholder data environment. Or, there are under secured systems that can access the cardholder data environment that are outside of the protected scope and, thus, creating risks. A common weakness is systems with connectivity into applications and databases that are not running with multifactor authentication (MFA). Under PCI DSS, all non-console access into the cardholder data environment must be secured with MFA but it's rare to see this level of control.

One area where I'm seeing people struggle—and rightly so—is restricting access based on business need to know. This concept is great, but it can be difficult to implement. This approach is especially challenging if you don't know who is supposed to have access, don't have proper buy-in from the various business units, or have no way of enforcing it. I would argue that implementing business need to know across your cardholder data environment is easier technically that it is operationally, culturally, and politically.

Of course, that could be said about many other things in security. Still, you must do what you can to strike a balance across all areas.

Another thing that I often witness is oversight and confusion related to which systems actually process cardholder information and whether or not the end client is responsible or it's the responsibility of an up/downstream third-party vendor. Furthermore, and for similar reasons, I see retail-based systems that are running extremely outdated operating systems and applications which furthers the security challenges, especially as it relates to truly locking down and controlling access in order to minimize exploits.

These risks are not just what I'm seeing in my work. They're also underscored by annual security studies. For example, the 2018 Verizon Data Breach Investigations Report found that application authentication attacks are prevalent in the financial and retail industries. As the report states "essentially the criminals are turning a PCI compliant application that does not store payment card data into a very non-PCI-compliant and criminal-controlled data harvester." Additional insight is provided by the 2018 Trustwave Global Security Report which found that the largest single share of security incidents involved in the retail industry—16.7%. Although a reduction from the previous year, it's still a troubling finding not unlike finance and insurance industry which made up 13.1% of all incidents. The Trustwave report also found that e-commerce systems made up the majority of all incidents affecting retail. On the financial side, it was corporate/internal networks where the majority of incidents occurred.

## More Than Compliance

I think many enterprises try to take the path of least resistance and most convenience when addressing authentication and access control. It's totally and completely understandable. I don't envy anyone who must jump through dozens of hoops daily just to access systems to get their work done, much less figure out how to do it for hundreds or even thousands of users. That said, a lackadaisical approach to authentication and access will likely prove to be indefensible in the eyes of the credit card brands, the PCI Security Standards Council, and other parties involved when a cardholder data incident or confirmed breach occurs.

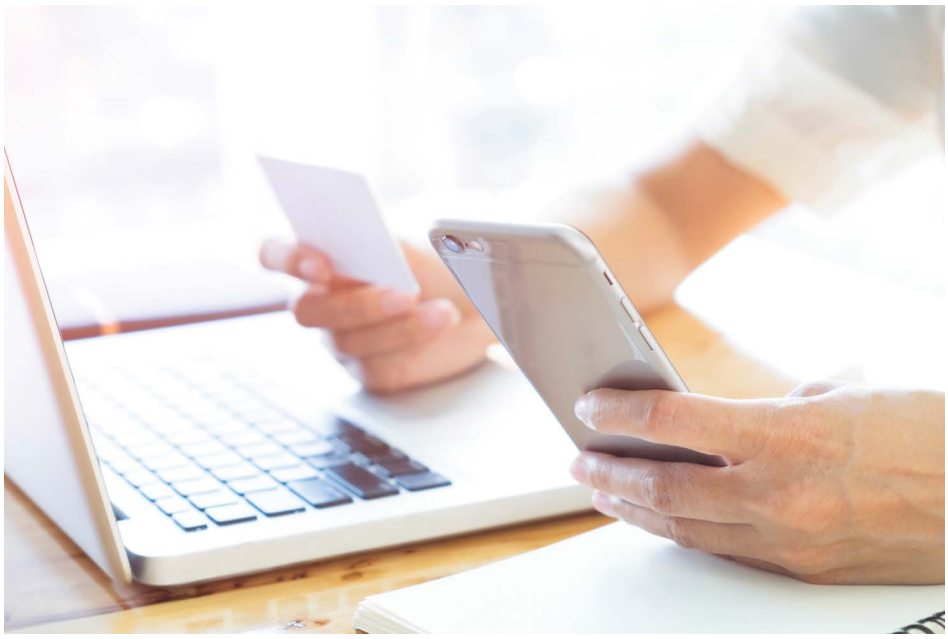
As with any other regulation, compliant does not mean secure. PCI DSS is a set of rules should be followed to the letter where it's reasonably possible and then go beyond that where you can. I've seen organizations in retail and financial services treating PCI DSS more as suggestions or best practices to shoot for. That's not a smart—or sustainable—approach. Security is a numbers game. When you combine the number of credit card transactions and number of cardholder records with growing information systems complexity, it's a matter of time before your controls are put to the test. Compliance is good, but security should be the goal.

Solid authentication and access controls applies to endpoints, network systems, and the core applications and databases themselves—whether mobile or in the cloud. I think the precedent that is being set by PCI DSS is:

- Does it meet the base security requirements?
- Is it properly implemented?
- What else can be done to make it better and further protect cardholder data?

But don't just let the PCI Security Standards Council fully dictate how you run your security program. These are also great questions to ask yourself to look for opportunities on a broader scale.

Minimizing PCI DSS-related risks goes beyond control and prevention. It also has to involve automated threat/incident response in order to quell the impact and actions of a threat on the cardholder data environment.



Contact us at **CyberRes.com**
Like what you read? Share it.

This could apply to a rogue user, such as a contractor with ill intent, attempting to gain access to point-of-sale systems. It can also apply to a malicious actor with stolen credentials and even malware looking to exploit credit card records—both stored or traversing the network in real-time. Where there's a lack of automation, there's a lack of insight. And lack of insight often leads to unnecessary security challenges.

Remember, with PCI DSS, the mandates are all about controlling access to cardholder data and being able to respond to incidents if they do crop up. I don't think perfection is expected. However, security controls mean nothing unless and until you determine your risks, document your policies and standards, and implement the proper technologies to see it all through in the right ways for your business. This is especially important in retail and financial services given the visibility of these industries and what there is to lose in terms of expansive amounts of credit card-related records.

Good security goes beyond PCI DSS Requirement 8 (Identify and authenticate access to system components) and practically everything else in that regulation. The important thing is to ensure that you truly understand where things stand and then take the necessary steps to keep things in check. At the end of the day, a low-risk cardholder data environment comes from a mindset of resiliency and a philosophy of common sense. Mostly, it's about discipline—doing what's right for the business rather than just doing what you're told.

**Written by Kevin Beaver, CISSP**
Kevin Beaver is an **independent information security consultant, writer, professional speaker, and expert witness** with Atlanta-based Principle Logic, LLC. With over three decades of experience in the industry, Kevin specializes in performing independent security assessments and consulting to help his clients uncheck the boxes that keep creating a false sense of security. He has authored/co-authored 12 books on information security including the best-selling *Hacking For Dummies* and *The Practical Guide to HIPAA Privacy and Security Compliance*. In addition, he's the creator of the Security On Wheels information security audio books and blog providing security learning for IT professionals on the go. Kevin can be reached at through his website at **www.principlelogic.com** and you can follow him on Twitter at **@kevinbeaver**.

784-000002-001 | M | 05/21 | © 2021 Micro Focus or one of its affiliates. Micro Focus and the Micro Focus logo, among others, are trademarks or registered trademarks of Micro Focus or its subsidiaries or affiliated companies in the United Kingdom, United States and other countries. All other marks are the property of their respective owners.

CyberRes
A Micro Focus Line of Business