

Playing by the (PCI) Rules

RSM McGladrey helps firms big and small stay secure and compliant

By Bryan Ochalla

Doing all that's needed to achieve PCI Data Security Standard compliance isn't easy—especially for smaller payments organizations, which often lack the internal resources necessary to meet the council's stringent guidelines.

Enter RSM McGladrey. Although the Minneapolis-based firm may best be known for offering accounting, tax, and financial services to the broader business world, it also helps the payments industry stay on the straight and narrow. Specifically, the company caters to merchants and service providers that are trying to become (or remain) PCI compliant with external network security scanning, penetration testing, assessments, remediation services,

and compliance validation reports. The company has 8,000 employees and 95 offices throughout the United States as well as international capabilities as a member firm of RSM International.

Merchants and service providers come to RSM McGladrey for many different reasons, according to Greg Schu, a managing director within the firm's technology risk management services department. Regardless of the reason, though, the conversation tends to start the same way each time.

"Our initial discussions are centered around what the client's environment looks like and where they may fall on the grid in terms of what they have to do to comply with the PCI requirements," he says.

Smaller Clients, Bigger Needs

It's increasingly common for Schu's team to work with smaller merchants and service providers—not only because there are more of them today than in the past, but also because such organizations are increasingly finding themselves under pressure from the PCI Security Standards Council to comply with its ever-changing requirements.

"You'd be surprised at how many companies have card information around the world," Schu says of RSM McGladrey's client base. "There are an amazing amount of Starbucks-like merchants out there as well—many of which are smaller than the coffee giant but still have enough transactions going through their systems that they have to be compliant, too."

In the early days of PCI DSS, smaller merchants and service providers were overlooked by the card brands and credit card processors, which took aim at the industry's larger players first. But that situation has changed, as evidenced by Schu's observation that "a lot of smaller

organizations are just now feeling the pressure" to become compliant, as well.

Smaller merchants and service providers come to RSM McGladrey for other reasons, too. "They may be increasing in size and may be coming up against some of the requirements and need assistance meeting them," Schu says.

Such organizations may have been able to get through the optional self-certification questionnaire when they were smaller, but as they've grown and become more complex as a business, "they now need assistance in terms of what they should be doing or what they should be looking for when trying to meet PCI compliance requirements," Schu says.

"They might read the requirements and think they know what they have to do [to meet them], but they come to us for assurance and ask, 'Can you help us through this? We don't understand what they're asking us for,'" he adds.

More than Bits and Bytes

Larger merchants and service providers also call on RSM McGladrey in general and Schu's team in particular, "especially if they have to do the full PCI report on compliance because of the number of transactions they do," Schu says.

"Even though the requirements say they could complete the report, have an officer sign off on it, and issue it themselves, many merchants and service providers ask us to assist them simply because they don't do this day in and day out like we do."

These clients may still complete a large chunk of the work themselves, but the company still helps with oversight because of its extensive understanding of the requirements.

RSM McGladrey has been helping merchants and service providers become PCI DSS compliant since the standards were first released in late 2004. Schu believes that thorough understanding of compliance experience, as well as the firm's history of working with the CPA firm, McGladrey & Pullen LLP, help differentiate it from its many competitors.

"We're not just a 'bits and bytes' company," he says. "We don't just tell our clients, 'That's what it says and that's the way it has to be.' The requirements aren't black and white. There isn't just one way to interpret and comply with them. They're kind of like tax codes: There may be multiple ways to comply with them, and each person probably won't comply with them in the same way." **TT**

Bryan Ochalla is a contributing writer to Transaction Trends. Reach him at bochalla@yahoo.com.

RSM McGladrey
Accounting | Tax | Business Consulting

"The requirements aren't black and white. There isn't just one way to interpret and comply with them."

—Greg Schu