

# Selling SECURITY

*Strategic ISOs turn seeming burden of compliance into a boon by offering added value to merchants*

By Bryan Ochalla

## KEY NOTES

- ▶▶ In helping merchants become compliant, ISOs can become “experts” and differentiate themselves as such among the competition.
- ▶▶ As more larger merchants become compliant, the crooks will consider the small merchant low-hanging fruit.
- ▶▶ Understand what your merchants are trying to accomplish and what their point-of-sale environment is. Then, recommend the right solution so they don’t find themselves painted into a corner.

Seven years ago, ISOs could go about business the way they always had: “They sold fairly simple point-of-sale (POS) terminal programs to vendors, and that’s about all there was to it,” says Cliff Gray, an associate with The Strawhecker Group, an Omaha-based consulting firm that targets the payments industry. “Sponsor banks or processors—whomever the ISO had a relationship with—provided support for the terminal and the application running on it,” he adds.

Data security was simpler, too. Terminals communicated over what were relatively closed networks that revolved around the telephone line.

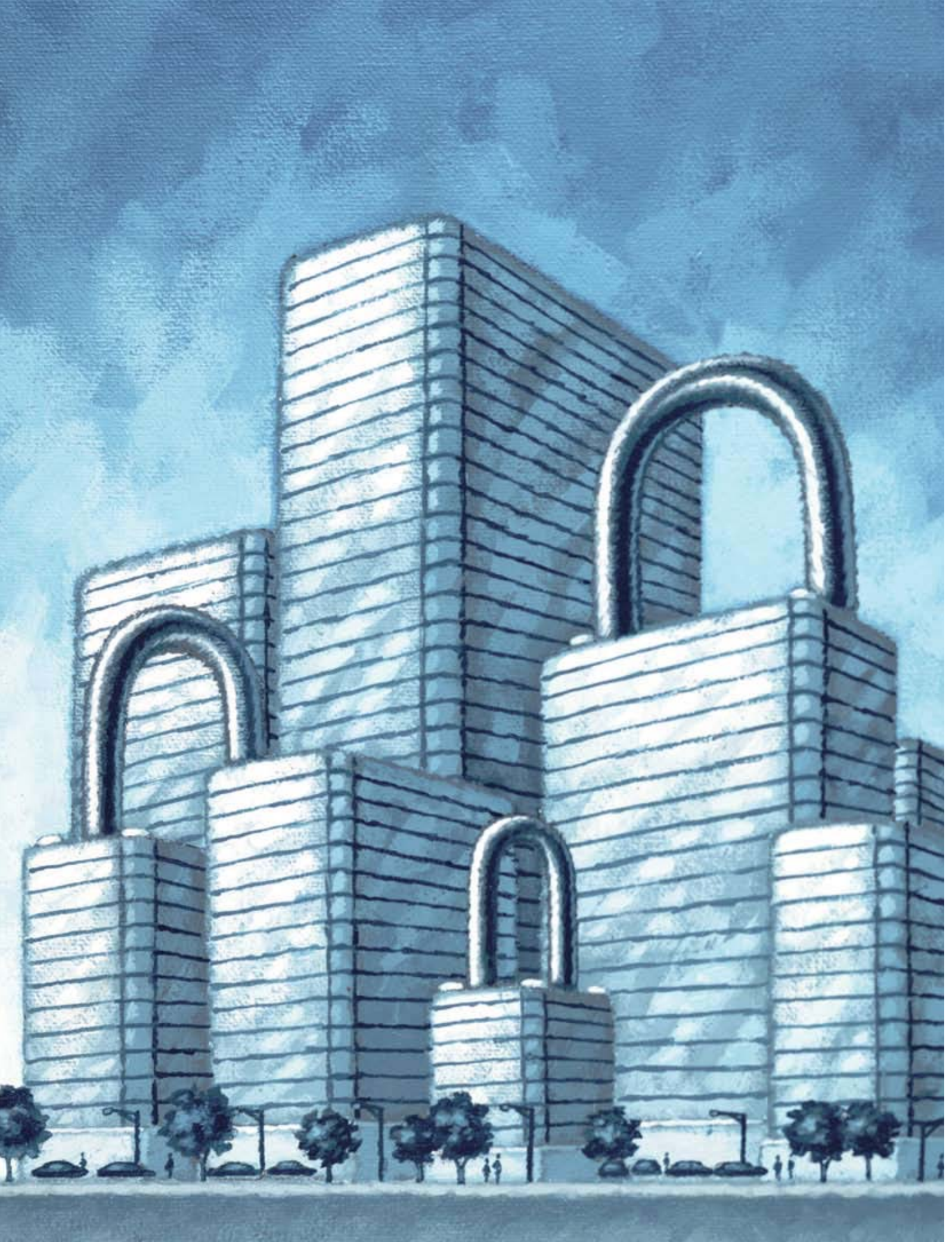
“As soon as we started pushing transactions over the open Internet, all kinds of schemes, scanning software, Trojan horses, and other mechanisms arrived on the scene to exploit the vulnerabilities of POS systems and capture and steal card data,” says Steve Mathison, vice president of POS

terminal and hardware solutions for First Data in Greenwood Village, Colorado.

It was that increasingly insecure environment—combined with a few (or more) high-profile breaches at large retailers—that led to the introduction of the Payment Card Industry Data Security Standard (PCI DSS) in late 2004. One of the main drivers of the standard, says Mathison, was that “as these transactions left the point-of-sale devices, we had to make sure we had the proper controls and security wrapped around them so the bad guys couldn’t see the data as it flowed through the Internet and use it illegally.”

Three years and one update later, PCI continues to loom over ISOs and merchants alike, many of whom who are struggling to catch up, let alone stay up-to-date. Although technology plays a role in the effort, Mathison and others suggest a little old-fashioned communication could help ISOs and merchants even more. Some ISOs are leveraging the compliance reality, work-

Eric Westbrook/images.com



ing with merchants to upgrade, and reaping strong customer loyalty in return.

### Educating Merchants on Risk

“ISOs basically only had to sell POS terminals,” Gray says of the industry’s pre-PCI period. “Now there’s so much more they have to be responsible for. This has been a huge paradigm shift.”

Now ISOs have to take steps they wouldn’t have even contemplated in the past. “There’s a much deeper level of communication that needs to happen between the ISO and their merchants,” Gray suggests. “In the past, they sold a terminal and then didn’t have much to do with the merchant after that as long as the transactions were flowing as expected.”

It doesn’t help that the PCI requirements are more than a bit complicated, suggests Mathison. If an ISO lacks a firm understanding of what the PCI requirements are, then “that makes it difficult to ensure that their salespeople are properly communicating that same information to the merchants,” he adds. “It’s a complicated subject, especially when you get down into the ‘weeds’ of having a terminal, a Wi-Fi router, and all the other things you need at the point of sale. Adding up all of those complexities and trying to stitch them together into a recommendation for a particular customer or location can be really difficult.”

Keeping his finger to the PCI pulse is how Chuck Saden, president of POS Card Processing in Cypress, Texas, dealt with that potential pitfall. “A few years ago, most of the concentration was on level-one and level-two merchants,” he says. “PCI compliance didn’t become our priority until it became apparent that level-three and level-four merchants would be expected to prove their PCI compliance as well.

“Once we found out that level-four merchants would be forced to prove their compliance, we started sending out a series of letters each month educating our merchant base on non-compliant software, along with the questionnaire for PCI compliance,” Saden continues. “We then started building our merchant base and setting them up with an approved scanner from the PCI DSS Web site.”

Although the company had to put some effort into that initial legwork, “once the merchants understood the issues of compliance and why they needed a scanning service, their response was very positive,”



**“A lot of merchants just don’t know any better. When they find out what’s at stake for their company and their customers, though, it really makes an impact.”**

—Matt Clyne, Senior Vice President, Sage Payment Solutions

according to Saden. “The amount of time and effort put into explaining PCI compliance has done wonders for lowering attrition. Merchants know that we care about them and are looking out for their best interests.”

Although Melville, New York-based EVO Merchant Services is a processor and not an ISO, the company publishes monthly PCI statement reminders to merchants that cover a broad range of topics. Compliance Officer Mark Brady believes that constant communication to merchants is critical, and many ISOs could benefit from copying EVO communication efforts, which include:

- directing merchants to Visa’s Web site for validated third-party software,
- publishing a Visa listing of non-compliant third-party software on the EVO Web site (merchant password required),
- requiring PCI validation for all level-three and high-risk level-four merchants,
- using password security best practices (never using a vendor-default password, changing passwords periodically, etc.), and
- practicing PIN pad security and best practices, such as mandating inventory control for PIN Entry Devices (PEDs), allowing only authorized personnel to

service and deploy PEDs, and training staff on PED security.

“We have also sent PCI-related correspondence to level-four merchants that are in the higher risk categories of restaurants and schools,” Brady adds, noting that approximately 60 percent of confirmed data-security breaches occur at restaurants. “We are making a concerted effort in 2008 to ensure that merchants using third-party software are not storing sensitive cardholder data.”

Sage Payment Solutions in McLean, Virginia, is another ISO reaping rewards from communication efforts with merchants. The company routinely prints out articles and other information related to PCI compliance—especially the ramifications of non-compliance—and delivers it to merchants.

“A lot of merchants just don’t know any better,” says Senior Vice President Matt Clyne. “When they find out what’s at stake for their company and their customers, though, it really makes an impact.”

One way the sales force at Sage assures that impact is by highlighting a few key lines in each article. “Anyone will read at least three sentences of an article,” Clyne says. “So I pick out a few of the most important ones—such as a quote from a TJ Maxx executive saying the company thought its bases were covered—and

**lúcy** didn't invent  
the Gateway.

**she perfected it.**

Introducing the future of payment gateway solutions.

**Let Us Connect You:** Cynergy Data's LUCY Gateway securely processes all forms of electronic payment—credit cards, PIN debit, checks, gift cards, EBT and signature capture.

Our reliable, flexible and secure gateway also gives you:

- Free software developer kit and integration support
- Transaction times of 3-5 seconds
- 24/7/365 technical support
- Intrusion detection and SSL encryption
- Residual Income for partners when your merchants use LUCY

[cynergydata.com/gateway](http://cynergydata.com/gateway)  **866.473.1349**

**lúcy** Gateway  
let us connect you  
A Cynergy Data Solution

highlight them. That really brings the message home.”

Although some may point the finger at the industry’s on-the-ground salespeople when asked who is to blame for the lack of understanding about compliance among level-four merchants, Clyne isn’t among them.

“This is something that has to be dealt with at all levels,” he advises ISOs. “If your salespeople aren’t ‘getting it,’ those in the upper levels of the company are partially responsible. Everyone needs to do a better job of educating themselves and others about this subject.”

Mathison agrees. “There has to be better idea transfer from the card associations to the acquirer to the ISO to the merchant-level salespeople—that’s the critical link in all of this,” he suggests. “The message can’t

The secret is to help merchants become compliant in a meaningful way. “I think there’s a way to position yourself as adding value to a customer,” Mathison adds. “Tell them you will make sure everything’s handled, and they won’t end up like TJ Maxx. Tell them you’ll give them the latest equipment, help them understand the rules, and just take care of them overall.”

But it’s not just a matter of throwing new technology at merchants. “You have to understand what your merchants are trying to accomplish and what their point-of-sale environment is,” Mathison says. “Then, recommend the right solution so they don’t find themselves painted into a corner.”

That was the approach of Sage Payment Solutions. “Some ISOs think of PCI compliance as a burden, but I think of it as an opportunity,” Clyne offers. “As a sales guy

comes knocking on their doors.

“Unfortunately, I’m not sure there are that many people on the street right now who have that level of expertise, and who can really roll up their sleeves and sit down with the merchant and talk about this.”

### Small-Time Service

One solution to that problem is to reach out to assessor companies that can help with the administrative portion of PCI. Such assistance comes at a price. “ISOs really have to assess, based on what they’re being asked to do, who they can turn to if they can’t do it themselves, how much it’s going to cost, and how much they’re willing to pay for it,” says Gray, adding that assessors may have to scale down their prices for it to occur.

“They may not see any ROI if they do that, though, just like the ISOs may not see any ROI out of it,” he says. “So, at some point, Visa and MasterCard or the sponsor banks may have to step up and provide financial incentives if they really want it all to happen.”

Visa and MasterCard may have to step up in other ways as well, suggests Mathison. So far, the focus of PCI has been on the “big boxes”—such as Home Depot, Target, and Wal-Mart—where the potential of exposure is seemingly greatest because of the huge numbers of cardholders flowing through their check-out lanes. But from a quantity perspective, most of the breaches are happening at the smaller retailers.

“There are more of them [smaller merchants], and the bad guys are quickly discovering they can’t hack the big boxes anymore,” he says. “As more and more of the larger merchants become compliant, there will be no more low-hanging fruit for the crooks to pick, and they will look elsewhere. Then, the low-hanging fruit will be the small merchant who simply hasn’t thought about this ‘security stuff.’”

Mathison says it’s something issuers, acquirers, and ISOs alike are going to have to think about for quite some time. “Eventually someone will find a way to breach even the latest PCI requirements. Once everyone is compliant, the bad guys will have a go at the overall shell and crack it, and then we’ll go through another round of PCI requirements. The key to combating that will be to remain eternally vigilant.” **TT**

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

## “There has to be better idea transfer from the card associations to the acquirer to the ISO to the merchant-level salespeople—that’s the critical link in all of this.”

—Steve Mathison, Vice President of POS Solutions, First Data

become garbled, and everyone involved needs to make sure that information flows all the way down to the merchant levels so they fully understand.”

“What really has to happen, among other things, is an educational process—from the acquirers to their ISOs—about how to pay attention to PCI and why,” Gray agrees. “Some of that is going on, but it doesn’t have teeth.

“It’s one thing for KeyBank to go yell at First American Payment, ‘Get all your merchants compliant!’ But if KeyBank doesn’t provide any real tools along with that request, it’s hard for the ISO to step up,” Gray adds. “They don’t always have the tools needed to accomplish the task, even if they understand the importance of doing so.”

### Understanding Merchants’ Goals

Even the best tools won’t work for ISOs that don’t have a deeper understanding of their customer merchants. “Most end-user merchants aren’t thinking about their point of sale,” Mathison says. “They’re too busy thinking about attracting new customers, positioning their inventory, or making payroll.”

myself, each time this process advances or evolves I see it as creating another opportunity for me to talk to merchants about what they need to be doing and how it will positively affect them.”

Salespeople have to tell merchants what ISO compliance means for them—whether that is keeping their customers safe or keeping their name out of the newspaper—but they can also use it to boost numbers.

“If your salespeople can become experts in this area, they’ll add value to the conversations they’re having with merchants,” Clyne says. “And if they add value to those conversations, they’ll get more sales.”

Mathison also sees positioning merchant-level salespeople as compliancy experts as a benefit to ISOs—at least for a while.

“Eventually, everyone will have to do it,” he says, “but in the meantime, the folks who find a way to take this complicated data and package it up in a way that merchants can understand will get them to think about the other good things they can do for them. And, it will give merchants one less reason to leave when another ISO