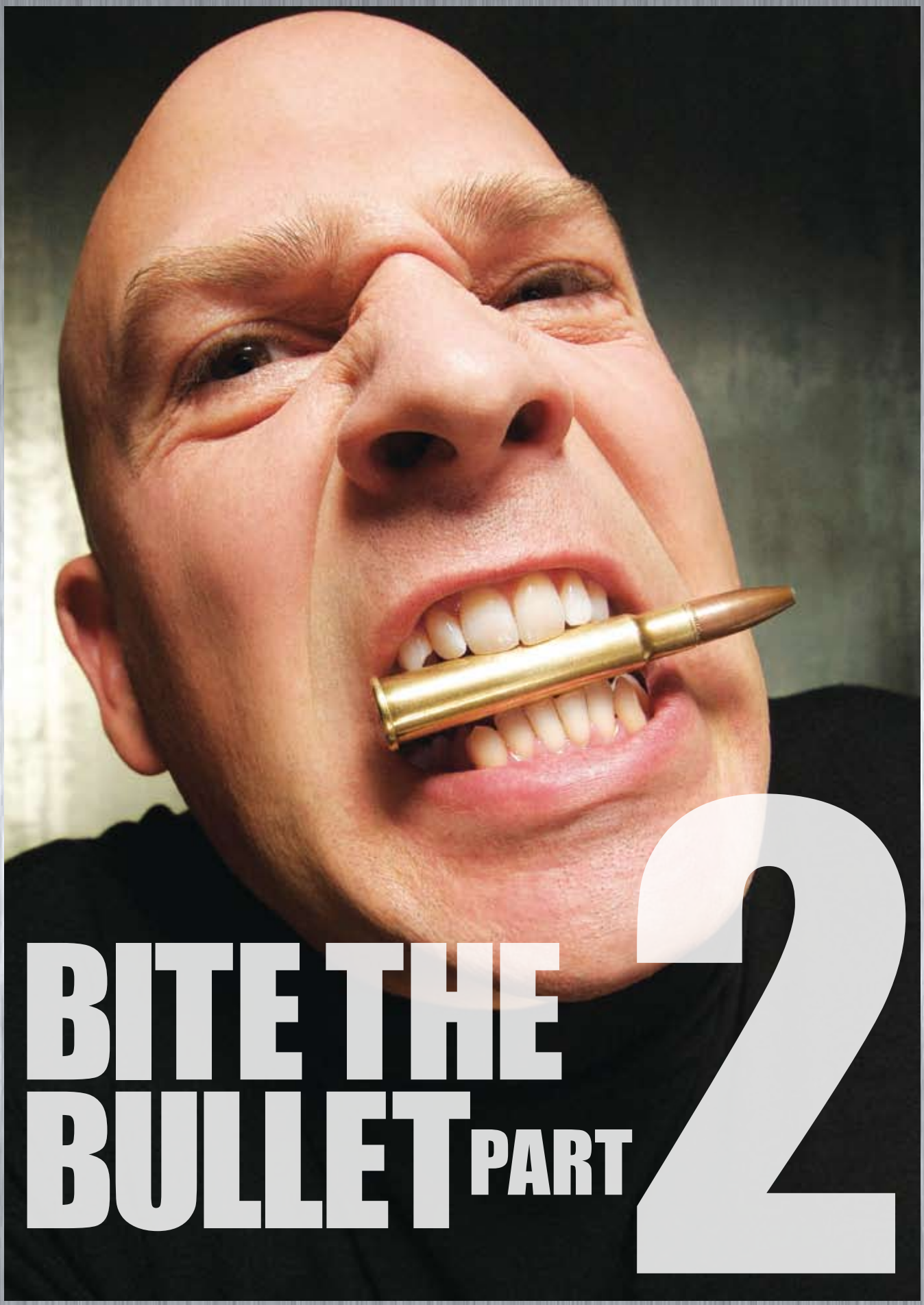


BITE THE BULLET PART 2

NOW YOU HAVE HELP! NACS stands up for your interests and makes sure that PCI compliance is as bearable as possible.

BY JERRY SOVERINSKY

Ironic.

How else can we characterize the impact on an industry whose promise to its customers is one of *convenience*, yet whose customers' preferred payment method — one predicated on *convenience* — is the one threatening its very survival?

Credit cards.

It's hard to imagine that an industry that can withstand a historic recession (one that has devastated other retailing segments) has found its Achilles heel in wallet-sized pieces of plastic. As one of the biggest issues facing convenience store retailers, credit cards are the focus of heated, ongoing debates at the state and federal levels, and whose inherent costs threaten to cripple retailers both big and small.

And no, we're not talking about credit card interchange fee costs — we're talking about the costs of PCI compliance.

PCI compliance (and data security in general) poses a more significant financial challenge for retailers, with potential financial penalties unmanageable even for the largest corporations. It's also an emotional issue for retailers, and understandably so since the mandatory requirements present a de facto loss of control for those whose day-to-day processes are ongoing exercises in self-determination.

And while imminent deadlines create a deepening sense of oppression, find reassurance in this: You're not alone.

No matter your sales volume, geographic location or the brand of fuel at your pumps, if you're a NACS member, your interests are top-of-mind and passionately represented by the association.

While you might wear many hats during the course of the day — indeed, **because** you wear many hats — NACS is standing up for your interests, making sure that PCI compliance is as bearable as possible and that it does not place unreasonable burdens on your operations.

So while you're wearing the hat of the manager, HR director and store greeter, here's what NACS is doing for you...

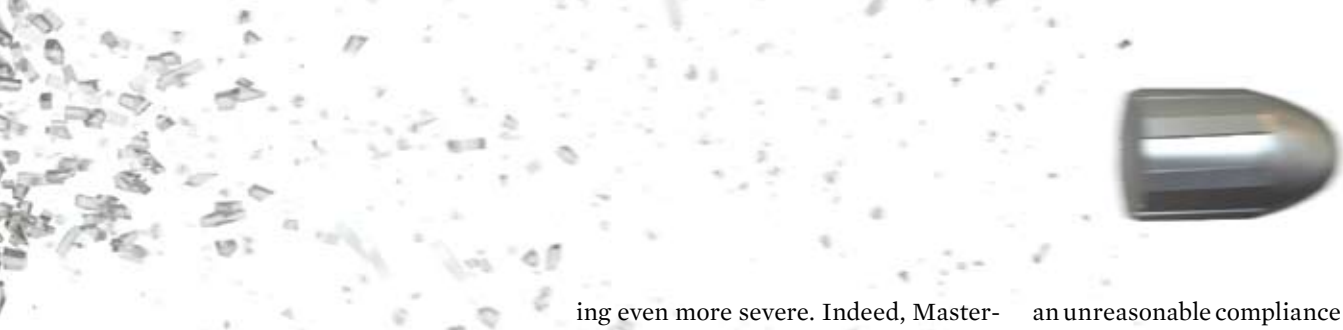
MONEY AND TIME

The most pressing PCI concerns for retailers are the cost and convenience of achieving compliance. NACS estimates the industry costs for 100 percent compliance at nearly $5 billion for PCI and triple data encryption standard (TDES) compliance, with non-compliance penalties boosting the total much higher.

"Should the small operator not comply, they run the risk of being assessed fines of up to $5,000 per store, per month and loss of card acceptance — in an industry with an average pre-tax profit of less than $4,000 per month," said Gray Taylor, cards payments consultant for NACS.

"Visa has confirmed to me that they have no intention of fining small operators out of business, but that attitude may change at any time, and MasterCard has not signaled its agreement with Visa," Taylor continued. "Further, there has been no softening by either brand when it comes to larger Level 1 and 2 merchants."

Larger companies in particular face burdensome penalties that are becom-



ing even more severe. Indeed, MasterCard has blurred the lines of Level 1 and Level 2 merchant compliance standards and penalties.

"MasterCard has unilaterally collapsed the requirements of Level 2 merchants to the more costly and stringent requirements of the largest Level 1 retailers," Taylor explained.

Retailers have stated that the entirety of their IT budget is dedicated to complying with PCI mandates — at the cost of postponing other IT initiatives that improve operating performance.

"Similarly, they have extended the larger fines for non-compliance. Before, a Level 2 merchant [around 150 convenience stores] could be fined $60,000 per year for non-compliance by each of Visa and MasterCard. After MasterCard's changes, [they are] now liable for fines up to $375,000 per year...along with the increased cost of complying with the Level 1 mandates," he said.

These penalties are sufficient to motivate action among all retailers, yet the hard costs of compliance are proving overwhelming.

"Several retailers have stated that the entirety of their IT budget is dedicated to simply complying with the PCI mandates — at the cost of postponing other IT initiatives that improve operating performance," Taylor said. "Further, the technical and security knowledge required to become compliant, along with the estimated $20,000 per store cost, is recognized to be a huge challenge for the industry's roughly 90,000 single-store operators who don't have the resources to easily comply."

And all of this is compounded by the hardship of meeting what for many is an unreasonable compliance timeline.

"The card brands have driven deadlines that are in most cases impossible to meet," said Drew Mize, vice president of product management and marketing at The Pinnacle Corporation.

"[The deadlines] have achieved nothing but continually erode [the industry's] actually meeting their requirements because [the card companies] constantly extend the deadlines and/or change the requirements before the prior set of requirements were met by any majority of retailers," Mize stated. "Retailers don't really know where the goalposts are so as a result we don't act and wait for the posts to be moved again."

TURBO TAX MEETS SAQ

Recognizing these challenges, NACS has invested significant effort on making compliance, especially for small retailers, meaningful, attainable and uncomplicated.

The solution targets PCI's Self Assessment Questionnaire (SAQ), a validation tool (which retailers complete annually and submit to their acquiring bank), that offers remediation guidance and best practices that ensure ongoing compliance.

While larger retailers are more capable of bearing the costs of PCI compliance, smaller retailers have been hindered by complexities and costs, especially in filling out the SAQ, which even for IT types can prove confusing.

"We have 93,000 Level 4 retailers — maybe even close to 105,000 — and filling out the SAQs is like looking at the [IRS] 1040 long form," Taylor said. "I've gone through the SAQs and they're challenging for me."

NACS approached several of the major oil companies at NACStech in May and made the case for a simplified, uniform solution — a TurboTax-like approach to the SAQ. The end result was announced in October at the NACS Show: NACS EZ PCI, which is a simplified, interview-based software solution for filling out PCI's Self Assessment Questionnaire.

Offered exclusively in partnership with Coalfire Systems, a recognized leader in PCI assessment services, NACS EZ PCI guides retailers through the SAQ process step by step. With a price tag of $119, this is a significant savings from recruiting third-party IT assistance, and down significantly — nearly 80 percent — from the early vendor quotes that NACS received.

"We've gotten our costs down from $500 a unit for a 'one size fits all' product to $119 for the compliance interview process that is specific to our industry and provides $50,000 of breach insurance; $149 including quarterly port scans to ensure hackers aren't coming through the back door, which is great for small retailers who are breaking even," Taylor said. "The last thing a small retailer can do is pay thousands of dollars [for compliance efforts]."

THE PURSUIT OF UNIFORMITY

Ensuring that your company is PCI compliant is complex enough. Add to that evolving state regulations in the absence of federal guidance, and it's no wonder the issue has many retailers gasping for relief.

To date, there is no federal law governing PCI compliance. However, some states have taken the issue into their own hands with legislative action. In 2007, Minnesota passed the Plastic Card Security Act. Earlier this year, Nevada enacted its Security of Personal Information law. Massachusetts is actively pursuing its own data protection regulation (201 CMR 17.00). Collectively, these piecemeal

DID YOU KNOW?

The NACS EZ PCI (Online SAQ) is available to NACS retail members for $119 ($169 for non-members) and NACS EZ PCI Plus (SAQ with quarterly report scans) is available for $149 ($209 for non-members). To order, visit nacsonline.com and click on "Shop" or call (800) 966-6227.

standards have NACS payment industry experts uneasy.

"Regardless of how merchants feel about PCI, it is at least a single standard that applies to the entire U.S. region,"

The Department of Homeland Security isn't sure it wants to take on credit card security, despite the fact that our president has said card security is a matter of "national security."

said Jim Huguelet from The Huguelet Group LLC, an IT consulting firm. "If this trend [states passing individual laws] continues, it will represent perhaps the worst possible scenario for merchants, resulting in a patchwork of state laws around payment security."

The result for retailers would be compliance with possibly conflicting laws, a costly administrative nightmare that would lead NACS to pursuing federal guidance.

"[A] single federal law that preempts the states might be the best possible outcome," said Huguelet, adding that it would allow NACS and the industry "to focus its education efforts into a single piece of legislation to make it as balanced as possible rather than having to try and do the same as part of dozens of individual states' legislative processes."

Currently, a federal approach is not being pursued aggressively by NACS, with most of its efforts concentrated on PCI compliance and data security.

"Right now, [pursuing a federal law that consolidates state law] is a side issue that we've just started," said Taylor. "Quite frankly, the Department of Homeland Security isn't sure that it wants to take on credit card security despite the fact our president has said card security is a matter of 'national security'."

NACS + PCATS → DSSC

PCI compliance and data security are ongoing concerns, with standards that require constant reassessments based on evolving technologies.

Recognizing this, in September, NACS partnered with the Petroleum Convenience Alliance for Technology Standards (PCATS) to form the Data Security Standards Committee (DSSC), a group dedicated to addressing data security-related issues.

"Card companies and PCI have issued far reaching security mandates to retailers, intended to help secure consumer card and transaction data," said Alvin Fortson, PCATS Electronic Business-to-Business Committee chair and director of systems development of the Pantry Inc.

"As retailers, we share the goal of providing our customers a safe and secure card payment infrastructure. This committee will further this goal by providing concise, cost-effective solutions [as] needed for retailers of all sizes to reduce and eliminate security risks," he said.

WHAT'S AT STAKE?

More significant for NACS members is not just PCI compliance, but data security. For as the Heartland breach illustrates (see sidebar on page 38), validated compliance does not equate with foolproof data security, and those suffering breaches cannot count on the card companies to stand in their corner. And in such a case, the most burdensome costs to retailers quickly come to bear.

"If there's a data breach and card numbers are lost with the security codes, the chance for fraud is almost 100 percent," said Rick Dakin, CEO of Coalfire. "And the [PCI] fines are the smallest part of it. It's all the chargebacks, the reissuing of cards that affects retailers."

The costs — both immediate and long-term — can be staggering.

"Losing just 10,000 cardholder records will cost a retailer nearly

$925,000 between fines, penalties, increased [and] instant audit needs," Pinnacle's Mize explained. "[T]here just aren't that many retailers that can afford this...not to mention a complete destruction of reputation."

Smaller merchants join NACS because they don't have specialized IT departments... somebody must be thinking in broad terms. And NACS is.

The bottom line for operations can be catastrophic and swift.

"Most of the merchants that we support suffer such a severe financial impact after a breach that 50 percent do not exist one year later," Dakin said.

ONGOING PURSUIT

Perhaps the biggest frustration with data security lies in its open-ended pursuit. Unlike interchange fees, which *could* be addressed with legislation, data security is and will always be an ongoing battle, an interminable cat-and-mouse chase that will forever resist closure.

"Cyber-security is here to stay. It's not so much PCI or government regulations; there's a mega-trend occurring, that we're much, much more reliant on our data systems," Dakin explained.

"Smaller merchants — they're just doing so many things every day, it's much more troubling. That's why they join NACS, they don't have time to have these specialized IT departments... somebody must be thinking in broad terms. And NACS is."

It's a committed effort, and one that continues to pay dividends for members.

"NACS [is leveraging] the combined buying power of many small operators to lower service costs and create easy-to-follow programs that facilitate compliance — just like it did with Card Processing Program," Taylor said. "Additionally, [the association continues] to educate the industry on how to become compliant as well as advocate within the PCI organization, card brands and regulators for a rational approach to achieving data security within our complex retail segment."

However, despite all of the efforts of NACS, data security still ultimately rests with its members.

"NACS and PCATS can't get retailers compliant, that's up to them," Taylor said. "We can only facilitate the process." NACS

Jerry Soverinsky is a freelance writer living in Chicago. He's also a NACS Magazine *and NACS Daily contributing writer.*

Remember Heartland?

In January 2009, Heartland Payment Systems, a credit card processor, announced that "malicious software" had breached its processing system in 2008. Reports called the breach the largest card data theft ever and estimated that up to 100 million cards had been compromised.

However, as a credit card processor, Heartland was subject to some of the most stringent data security standards, and during its most recent audit prior to the reported breach *and as reported by Visa*, it had successfully passed its assessment.