Limited-Service, Unlimited Possibilities

QSR® SmartChain

SIGNATURE SYSTEMS, INC
PDQ
RESTAURANT POS

PROGRESSIVE PAYMENTS

Navigating the new world of POS security

A New Way to Pay | EMV Simplified | PCI and Beyond

INGENICO

Chick-fil-A SECURITY BREACH	Dairy Queen SECURITY BREACH	Rainforest Cafe SECURITY BREACH	PF Chang's SECURITY BREACH	Morton's SECURITY BREACH
Chart House SECURITY BREACH	Bubba Gump Shrimp Co. SECURITY BREACH	McCormick & Schmick's SECURITY BREACH	Landry's Seafood SECURITY BREACH	Mitchell's Fish Market SECURITY BREACH
Vic & Anthony's SECURITY BREACH	Oceanaire Seafood Room SECURITY BREACH	Claim Jumper SECURITY BREACH	Mastro's SECURITY BREACH	Golden Nugget SECURITY BREACH

AWAKE AT NIGHT WONDERING IF YOUR ENTERPRISE IS NEXT?

SIGNATURE SYSTEMS SECURITY: a SOLUTION for SOUND SLUMBER.

Regardless of whose POS you have...

SIGNATURE SYSTEMS, INC
PDQ
TECHNOLOGY SERVICES

WE PROTECT YOUR DATA—AND YOUR BRAND— with a proven, comprehensive cyber-security solution for your *entire* environment.

Finally, iron-clad *restaurant-centric* protection that's simple and fast to deploy—
and takes no effort on your part to manage!

877-968-6430

PDQpos.com | PDQtek.com | PDQsecurity.com

We Eat, Breathe & (Soundly) Sleep Security

Securing Data Streams

PCI compliance and security in the new world of big data

Restaurants have a lot on their plates trying to achieve PCI compliance.

Now, with the Federal Trade Commission holding franchisors accountable for breaches that happen within the franchise community, data security *has* to be a top priority among restaurant brands. And within the scope of the new rules, a brand is only as strong as its weakest link.

Unsecured locations, however, are only one piece of the puzzle.

Basically, there are five key areas of data security vulnerabilities: weak firewall solutions, incomplete PCI compliance solutions, unsecured locations, weak remote access, and lack of employee training.

As for the last aspect, it's important to note that just as entire brands can be held liable for one lagging location, entire restaurants are held liable for one lagging employee. The PCI DSS requirement states all employees must be trained annually and upon hire on how to properly handle the customer credit card data. If a breach occurs and even one employee isn't trained, the merchant will be held liable for the breach.

There is more than one way to make sure comprehensive security is achieved.

Securing POS systems that are "in scope" can be difficult. In the past with magstripe readers, payments were processed in a fully integrated (in scope) environment, which means that all of the information from the magstripe reader was held within the POS software.

With all of that sensitive information shared throughout the system, restaurants are required to get every piece of the system PCI compliant. The problem with this is that every time a restaurant changes its software, each part the system has to be re-certified, creating extra steps any time a restaurant is looking for an upgrade.

This has led many restaurants to seek more options that are only semi-integrated.

In a semi-integrated system, instead of the sensitive information being shared between the magstripe reader and the other payment device, the POS terminal triggers a transaction and sends only the dollar amount and other non-sensitive transaction information to the payment device.

Finally, there's a standalone approach with no connectivity at all, wherein sensitive informa-tion is isolated in the payment terminal and the employee at the register simply has to manually enter the transaction amount on the POS.

There are benefits and risks inherent within every strategy. The key is to find a security partner to support whichever program best suits your business model, and then leverage their resources to ensure streamlined security compliance that addresses any and all areas of vulnerability.

This emphasis on providing enhanced security for cardholder data has been the latest secu-rity push in the restaurant industry. But with new programs and services, cardholder information is not the only information being collected from customers in restaurants.

According to the National Restaurant Association (NRA), more than half of consumers already use their smartphones and mobile devices to redeem rewards or participate in digi-tal loyalty programs.

That being said, it might be high time to consider upgrading from the punch card system. But this mass data collection of everything from detailed dining habits to birthday information has risks as well as rewards.

One of the emerging threats is around 'beyond-PCI data' that's coming in through customer loyalty programs.

Whether it's mobile ordering or trying to personalize the customer experience by gathering information on participants' habits, customers are inputting much more than the information on their credit cards. This information is often pro-vided under the assumption that restaurants are appropriately protecting all of the personal information that gets transferred, some of which is banking data tied to loyalty applications, and some of which is simple identifiers such as the customer's name, address, phone number, or dining habits.

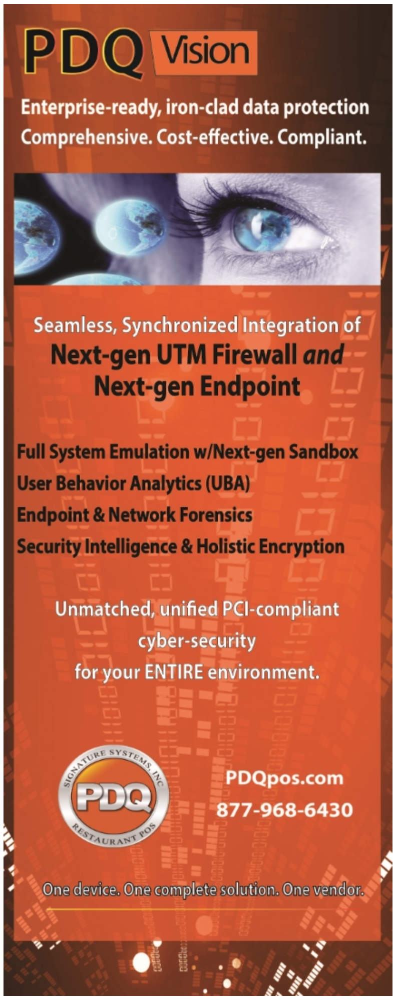
According to a 2012 report from the FTC, "many consumers are concerned about the privacy of their personal information" but "generally lack full understanding of the nature and extent of this data collection and use."

Similarly, the Department of Commerce released a consumer data privacy report stating "privacy protections are critical to maintaining consumer trust," but "neither consumers nor companies have a clear set of ground rules to apply in the commercial arena."

Clearly, this is problematic for all parties involved.

Being able to put a broader security control program around all sensitive data coming into a location is critically important, especially right now, when the protective controls around this extra data are not typically as strong as those around cardholder information.

Beyond-PCI data represents an emerging security threat



Signature Systems also recognized this gap in security and made the decision to tackle the problem head-on within its PDQ POS system.

"Our holistic, comprehensive solution goes beyond fraudulent card transaction—the PCI part of security—as it extends to sensitive customer, employee, and store data that resides on the net-work, server, and back-office PC,“ says Larry Fiel, marketing director. "And that's where data breaches occur. That's why we won't sell a POS system without completely securing a store's entire environment. After all, why lock the front door and leave the back door wide open?"

To attain this environment of total cyber security, Signature Systems created "PCI in a Box",which contains compliant EMV card-processing units, and PDQ Vision, with next-generation Unified Threat Management (UTM) hardware, synchronized next-generation Endpoint software, and a multi-tiered Unified Security Intelligence platform.

"We can protect your sensitive business and customer information with next-generation, end-to-end threat management and forensic intelligence. Our holistic solution offers complete security visibility and the acceleration of zero-day threat detection, incident response, and compliance management," Fiel says.

"The financial and brand-loss liability from a data breach is a recurring nightmare for those in the C-level suite," says John White, Signature Systems chief security officer. "The costs of los-ing sensitive and confidential information to hackers–both external and internal–increase annually, not to mention the long-lasting adverse effects of a tarnished reputation. Safeguarding sensitive personal information is just as vital as securing PCI-related data."

The company's goal is to educate restaurants about PCI compliance and help brands success-fully traverse the path toward data security.

As restaurants and consumers continue to reap the benefits of increased information sharing and personalized marketing, a new frontier for security is emerging around this information.

By partnering with a company that can ensure security beyond PCI compliance, restaurants can handle the burden of this new information gracefully.

In the process, it's likely that customers will discover even more reasons to be loyal to well-protected businesses.

Help Arrives For EMV

EMV tech is knocking at the door

When it comes to EMV adoption, U.S. restaurants have been late to the table compared to international concepts and the retail sector.

The liability shift from credit card issuers to restaurant owners for reimbursing fraudulent expenses went into effect on October 1, 2015, and companies scrambled to ensure that both payment hardware and software were EMV compatible in anticipation of the mass migration to the new technology.

That shift in the restaurant sphere, however, has been less dramatic than many manufacturing companies initially anticipated.

It's likely that the technology rollout in retail went much more quickly because of the relative homogeneity of that market, as opposed to the great variety of service and transaction styles within restaurants. EMV technology, for instance, is not the easiest thing to swallow for a quick-service concept that thrives on speedy throughput.

EMV transactions can take as long as 35 seconds to process. If a restaurant's previous transaction time fell somewhere between 7–10 seconds, this jump can give operators serious pause about adopting the new system.

Beyond the cost of lost time, there is also the initial equipment cost.

However, it is becoming more clear to many brands that the benefits of bulking up safety measures surrounding credit card transactions far outweigh the costs in the long run.

The walls of resistance are finally coming down in the U.S. because restaurateurs are being hit with liabilities and restaurants realize they have to do something about it.

In addition, this consumer knowledge has also led to some unfortunate instances of fraud where a customer has rung up a large bill knowing the restaurant doesn't have an EMV-enabled device and then denying the magstripe reader charge to their bank later, leaving the restaurant with no leg to stand on and a huge bill to foot.

Typically, POS and payment terminal companies provide EMV-enabled systems by connecting with a third-party "gateway service" that charges a small fee per transaction for the security it provides.

The U.S. is the source of around 20–25 percent of the world's card-present transactions, but is responsible for over half of the world's card-present fraud

Mike Reinecker, marketing director at Signature Systems, says, if merchants don't adopt it soon, consumers are going to start seeing them like the old-school guy on the block who still only accepts cash.

"Don't be afraid of doing it; it's going to save you money," he says. "It may cost you money upfront, but it's going to save you money in the long run in chargebacks and fraud, plus your customers are not going to be comfortable when they walk in and you're still sliding cards instead of inserting them."

Reinecker also thinks there are EMV improvements to look forward to in the future—from tip-enabled readers to mobile EMV. While taking EMV mobile has been less of a problem for quick-service restaurants, where customers typically pay at the counter anyway, the chip-and-pin process has been difficult to adopt when the service model includes taking the card away from the customer or allowing pay-at-table options.

Additionally, the new process affects classic tipping models. Some credit cards with EMV chips allow for tipping. With others, though, tips must be included before the initial card insertion and cannot be added after the fact. Another subset allow tips to be added, but only while the card is still in the terminal, which means that the customer must be standing at the register to input this information, limiting flexibility in payment taking.

"Intuitive software for EMV reading exists, and it's only going to get better around things like tip adjustment and processing times," **Reinecker** says.

EMV is only getting more convenient, and the threat of chargebacks is only getting larger. In this environment, opting out of this new, protective technology is a risky choice to take, even though implementation is likely to come with some hiccups.

f your business is still straddling the fence on EMV adoption, discussing options with a forward-thinking provider can do nothing but bolster your understanding of the costs and benefits of adding EMV to your tech roster.

EMV innovation is improving implementation and service times

Signature Systems
760 Veterans Circle
Warminster, PA 18974
877-968-6430
PDQpos.com

For more than 30 years, Signature Systems Inc. has been a leader in providing top-rated point-of-sale systems to the hospitality industry. Its feature-rich, blazing fast PDQ POS software is both powerful and easy to learn and operate. Fully customized to each user's needs, PDQ POS handles online ordering, pickup, delivery, takeout, walk up, drive thru, table service, and bar better and easier than any POS in the industry. PDQ POS comes with complete PCI-compliance and cyber-security package—one that keeps the POS safely "out of scope" and protects a store's entire environment.

Chick-fil-A SECURITY BREACH	Dairy Queen SECURITY BREACH	Rainforest Cafe SECURITY BREACH	PF Chang's SECURITY BREACH	Morton's SECURITY BREACH
Chart House SECURITY BREACH	Bubba Gump Shrimp Co. SECURITY BREACH	McCormick & Schmick's SECURITY BREACH	Landry's Seafood SECURITY BREACH	Mitchell's Fish Market SECURITY BREACH
Vic & Anthony's SECURITY BREACH	Oceanaire Seafood Room SECURITY BREACH	Claim Jumper SECURITY BREACH	Mastro's SECURITY BREACH	Golden Nugget SECURITY BREACH

AWAKE AT NIGHT WONDERING IF YOUR ENTERPRISE IS NEXT?

SIGNATURE SYSTEMS SECURITY: a SOLUTION for SOUND SLUMBER.

Regardless of whose POS you have...

SIGNATURE SYSTEMS, INC
PDQ
TECHNOLOGY SERVICES

WE PROTECT YOUR DATA—AND YOUR BRAND— with a proven, comprehensive cyber-security solution for your *entire* environment.

Finally, iron-clad *restaurant-centric* protection that's simple and fast to deploy—
and takes no effort on your part to manage!

877-968-6430

PDQpos.com | PDQtek.com | PDQsecurity.com

We Eat, Breathe & (Soundly) Sleep Security