SMART CHAIN

FEBRUARY 2018

VENDOR RESOURCES / TRENDS / NEW PRODUCTS

Limited-Service, Unlimited Possibilities

QSR

PAYMENT PROCESSING

As the digital landscape becomes more complex, so does handling digital payments. BY DAVINA VAN BUREN

THINKSTOCK

Merchant Solutions

Payment processing is having growing pains, but the future looks bright.

Admit it: You still hesitate when you pay with a credit or debit card. Do I swipe? Is there a chip reader? Do I enter my PIN? Do I need to sign?

This chronic confusion is one of the biggest challenges American consumers face, and one of the most common complaints in the quick-serve industry. In 2015, the U.S. began converting from swipe to EMV—Europay, Mastercard, and Visa, referring to a global standard for cards equipped with computer chips and the technology used to authenticate the transactions in which they are used. Since then, companies have gradually implemented the EMV system as costs allowed. Switching to new technologies and processing systems can be expensive, so larger restaurant chains were the first to adapt, while many mom and pop operations have yet to convert. But cost isn't the only thing that matters.

"Customers are getting more and more used to inserting their cards versus swiping," says Ray Moorman, vice president of product and integrated payments at **Vantiv**, "but it still causes some level of hesitation during the transaction, as the customer may be unsure whether to swipe or insert the card." That few seconds of hesitation and having to figure out which system your establishment is using may not seem like much, but multiplied by hundreds or even thousands of transactions per day, adds up quickly in terms of labor costs and drops in customer satisfaction.

Europe, Canada, and some other regions moved to the EMV system several years ago. Joe Zielinski, senior hospitality specialist at **PAX**, says the slow adoption path that the U.S. has been allowed to take regarding EMV has had a negative impact upon quick-serve operations, particularly on speed of service. "The sooner the quick-serve industry in the U.S. can get commonly onboard with EMV, the sooner it will avoid the consumer confusion that has plagued those retailers who thought early adoption of EMV hardware would be advantageous," he says. "In Canada, where EMV has been in place for the past seven years, the quick-serve industry across all brands has not only accepted it, but embraced and perfected it, even in drive thrus. This not only maximizes speed of service, but payment security as well," he says.

Key elements to solving this dilemma are education for restaurant owners, man-

THINKSTOCK

"Merchants need to educate themselves on why and how this will help their current state of payment processing and what safeguards need to continue after this new technology is in place."


Verifone

agers, and employees, plus proper signage. "The first step is education and not relying on your POS provider or merchant processor to drive you to a solution based on the new technology," says Mark Cline, a vice president at **Netsurion**. "Merchants need to educate themselves on why and how this will help their current state of payment processing and what safeguards need to continue after this new technology is in place." Employees should also be able to quickly and knowledgeably guide customers through the transaction process, and, when possible, signage that instructs guests to insert their EMV-enabled chip cards as opposed to swiping should be clearly visible.

As for drive thrus, the U.S. has a long way to go to catch up with countries who are further ahead in the payment processing game. "The payments industry and quick-serve restaurants have been designing acceptance solutions that address card entry challenges at drive thrus," says Tor Opedal, vice president of North America QSR for **Mastercard**. "Contactless or 'tap-and-go' solutions—cards and mobile devices—seem to offer the best choices." Another option is to send employees out with a mobile POS device to take orders directly from guests when lines get long.

Another growing payment method is near-field communication (NFC). Soon, consumers won't need cards at all, because NFC allows users to simply wave their smartphone over a compatible device to process payments. Services such as Apple Pay, Stripe, Samsung Pay, and even Bitcoin are changing the way consumers think about and handle money. "Apple Pay is reporting more than 1 million new users each week," says Joe Mach, president of **Verifone** North America. "Popular cloud-based wallets, such as WeChat Pay and Alipay, are breaking down borders and disrupting the payments ecosystem. User adoption will continue to increase, and payment providers and businesses need to prepare to accept a growing number of alternative payments."

As smartphone use spreads to the furthest reaches of the globe, new users are quickly adapting to this new way of doing business. Whereas credit and debit card transactions were once primarily used for shopping, today's foodies can use their smartphones to peruse menus, order online, and pay online, all from the palm of their hands. "Globally, some five billion people will be connected via a mobile device by 2020, ushering in mobile payments and removing the need for cash," says Terry Angelos, senior vice president of commerce solutions at **Visa Commerce Solutions**.

Another advantage to mobile payments is that they can be integrated into an omnichannel strategy for brand unification and engagement. Consumers increasingly have their smartphones at the ready

VERIFONE

to aid their purchasing decisions—whether to compare menu items or to find deals and locate products as they walk store aisles in real time. "Connecting both channels can provide them with access to the advanced consumer data and analytics needed for better targeting, consumer insights, and personalization across all customer touch points," Mach says.

"I think we could see a change to cardless transactions and move into a biometrics-type payment system or unique identifier for each consumer tied to their virtual bank account."

While full-service restaurants have seen an increase in pay-at-the-table solutions, quick serves have not—yet. "For quick serves, we typically don't see there being much adoption for traditional pay-at-the-table solutions because they require a server to bring over the device to help the guest check out," says Ben Wagner, director of solutions for **Ingenico**. "However, solutions where a tablet and mobile card reader or smart terminal are attached to the table could be a good fit, since guests could use it to place their order and pay, then pick up their food when their number is called without having to wait in line."

One important distinction in the U.S. is that pay-at-the-table technology is not required to accept EMV. "Restaurants can perform the same portfolio and receipt tip flows with EMV on the server station," says Marc Castrechini, VP of product management for **Cayan**. "However, benefits like improved customer experience and faster table turns have inspired restaurants to look into pay-at-the-table solutions."

With the proliferation of connected, payment-enabled devices ranging from cell phones to smartwatches, the quick-serve industry is focused on how to ensure safety and security at the point of sale. As alternative payment methods become more common and as unprecedented growth in the digital payment space continues, security will become even more necessary and will need to evolve. Traditional authentication methods such as passwords, Angelos says, simply aren't designed for the new ways people are shopping and paying, adding that Visa is constantly exploring new avenues to authenticate through the use of alternative authentication tools like voice and fingerprint recognition.

"At some point in the near future, I think we could see a change to cardless transactions and move into a biometrics-type payment system or unique identifier for each consumer tied to their virtual bank account," Cline says.

As consumers become more educated about security and the reasoning behind new payment technologies, like decreasing the risk of fraud, the need for secure and updated systems is more important than ever. "As quick-service restaurants move to 'card not present' environments, they need to take additional safety and security precautions lest they become prone to fraud," Opedal says. "There are two approaches that may be helpful: aligning with a security solutions provider that handles all networks and form factors on behalf of the merchant, or plugging into API (application programming interface) safety and security solutions offered directly by card networks."

Payment processing has significantly evolved in recent years, from "swipe" to "dip" and now "tap-to-pay" through contactless payment systems. The next step in that movement seems to be a further shift toward a cash-free environment, but restaurants who are still on the swipe system shouldn't fret. Today's technologies are being built to adapt to the quickly evolving payments landscape.

"It may not be what everyone is talking about, but it probably should be," Zielinski says, referring to the affordability of higher-end, faster EMV and NFC payment terminals. "They have the speeds, capabilities, and durability that would ensure maximum lifespans with minimum total costs of ownership. The payment terminal solutions that are available today have all the technologies built into them that will enable all known secure e-payment types for many years to come."

With the continued rollout of EMV, NFC, mobile ordering, and loyalty programs across the competitive quick-serve industry, owners who are willing to invest in the latest technologies—as well as find ways get to know their customers' spending habits better—can not only deliver efficient and secure payment experiences for their customers, but they can also increase their bottom lines. SC

THINKSTOCK

Security Solutions

Data security solutions aim to protect both the consumer and the merchant.

Recent years have seen a bevy of high-profile data breaches, including at Equifax, Arby's, Wendy's, Chipotle, and many more. The wide range of targets shows that no sector is safe from security threats—not even governments.

With the rise in mobile wallets and card-not-present environments, security is top of mind for restaurant owners and managers, as well as consumers. Data breaches can be disastrous for public relations and cause permanent brand damage.

"Consumers are more educated and more aware than ever of their personal and financial data, and restaurants need to be mindful of this," says Mark Cline, a vice president at **Netsurion**. Thankfully, a movement toward education and stringent PCI compliance is under way within the quick-serve industry.

"What has evolved since the start of the PCI (Payment Cards Industry) Security Standards Council, roughly 10 years ago, is a focus on strategies to devalue and desensitize cardholder data in merchant environments," says Tor Opedal, vice president of North America QSR for **Mastercard**. "Through technologies such as EMV chip, point-to-point encryption, and tokenization, businesses can successfully devalue and desensitize its cardholder data so that it is useless to criminals."

The first and most important step to ensuring the security of payment data is remembering the golden rule of PCI compliance: If you don't need it, don't store it. "Hackers cannot compromise data you don't have in the first place," he says. "There is no need, nor is it allowed, to store data from the magnetic stripe on the back of a payment card, or equivalent data from a chip."

THINKSTOCK

The U.S. is the last major market still using the magnetic-stripe card system, but recently there has been a push for conversion to EMV chip cards. Unlike magnetic-stripe cards, when an EMV card is used in a transaction, the card chip creates a unique transaction code that can never be used again. U.S. card issuers are increasingly migrating to EMV technology, both to address eroded consumer confidence and to protect themselves and businesses against fraud costs. Although EMV technology can't prevent data breaches from occurring, it does make it much harder for criminals to successfully profit from stolen data.

"Recently, trends in thinking about payments have gone from awareness about EMV to action for most merchants, which is a good thing," says Ray Moorman, vice president of product and integrated payments at **Vantiv**. "Accepting a compromised card can cost merchants thousands of dollars if they are not EMV-enabled,

"Consumers are more educated and more aware than ever of their personal and financial data, and restaurants need to be mindful of this."

while suffering a data breach can cost a merchant their brand reputation and potentially their business."

So far, the push is working, thanks in part to new regulations regarding card-present fraud. In October 2015, liability shifted to whichever party is the least EMV-compliant in a fraudulent transaction. Since the introduction of EMV chip cards in the U.S., both Mastercard and Visa have reported a dramatic decrease in fraudulent charges.

Another security option is tokenization, which replaces sensitive data with unique identification symbols that retain essential card information without compromising security. "Format-preserving tokens look similar to credit card numbers and will pass a credit card 'mod-10' validation, which makes them much easier to store in systems that were accustomed to storing card data," says Pete Cavanagh, vice president of sales at **Merchant Link**. "Good token services will maintain the last four digits of the original card so that it can be used as a reference and printed on receipts."

"Accepting a compromised card can cost merchants thousands of dollars while suffering a data breach can cost a merchant their brand reputation, and potentially their business."

Businesses work with a token provider who stores your customers' sensitive payment credentials, so "be sure to choose an enterprise-grade vendor with many years of experience doing this, and a long list of references of major name-brand merchants that have entrusted them to provide cardholder tokenization services," Cavanagh says. "A merchant-friendly vendor will work with you if you sell your business or choose to move to a different provider."

Businesses should also make sure their POS systems are secure. "Oftentimes when you hear about a data breach, people assume that it's the smart terminal on the countertop that's been compromised, but in reality the source of vulnerability is usually the POS system or the merchant's backend systems through which the card data passes or is stored," says Ben Wagner, director of solutions for **Ingenico**. "However, even in the event of a hack, tools like point-to-point encryption can help ensure that even if the data is accessed, it is unreadable. Other options include deploying your payment system in a semi-integrated configuration, which routes the sensitive cardholder data directly to the payment processor so that the POS never comes in contact." This differs from fully integrated POS solutions, where both the POS and the payment terminal can "see" guests' sensitive EMV information, its encryption, and its tokenization.

Finally, quick-serve merchants should ensure they have a multi-layered security system that protects sensitive information as it travels through the payment ecosystem. This means not only converting to EMV, but also pairing it with encryption, tokenization, and strong network security services, such as managed firewalls and network segmentation. While none of these measures alone make a merchant PCI compliant, they can greatly reduce friction in the card data environment and ease the PCI audit process. Merchants should also make sure they stay PCI compliant. "What most merchants don't know is the work it takes to become and stay PCI compliant," Cline says. "It is hard work, and it never stops. Adopting new payment security technologies will reduce the scope of your PCI compliance, but that does not make you compliant. There is still work to be done every week, month, and year."

Merchants should use security providers to augment their cybersecurity efforts, but they should also be educated buyers of such services and remember that outsourcing doesn't free them from the responsibility of protecting the data entrusted to them. SC

THINKSTOCK

Mobile Wallets Redefining the Payment Ecosystem

New payment technologies not only increase security, but also provide valuable consumer insight.

As the push for EMV continues, quick-service merchants and card companies are already looking to the next frontier in payment technology: mobile payments.

In 2017, ACI Worldwide reported that 17 percent of U.S. consumers now regularly use their smartphones to pay, up from six percent in 2014. Here's how it works: mobile payments, sometimes called digital wallets, use near field communication (NFC) to process financial transactions, among other functions. Essentially, NFC is technology that allows two devices, such as your smartphone and a payment terminal, to communicate with each other when they are in close proximity. There's no swiping or chip insertion involved. If you've ever used your iPhone to send photos or contacts using AirDrop, you've used NFC.

Ben Wagner, director of solutions for **Ingenico**, says restaurant leaders and consumers are looking toward contactless options, including NFC-based mobile payments like Apple Pay and Android Pay. "Contactless transactions reduce the time it takes to pay and makes the process more seamless," Wagner says.

Not only is this advantageous for the consumer, but it can also save on labor and reveal valuable consumer insight.

"Simple loyalty programs have always offered insight into customer behaviors, but emerging technology now helps business owners better understand customer experiences in real time and offers immediate and actionable insight," says Marc Castrechini, VP of product management for **Cayan**. "Among these solutions are easy single question ratings during checkout, consumers interacting on their mobile wallets after a transaction, and even social media profiles."

THINKSTOCK

Furthermore, Castrechini says once the groundwork is laid for mobile payment and loyalty, much of the same technology can be used for mobile discounts and offers, allowing consumers to see the benefits of loyalty more quickly and easily than ever before. "This is extremely powerful," he says. "Mobile wallet providers can use offers platforms and maps capabilities to bring new customers into restaurants that they may not have otherwise visited."

Looking even further into the future, mobile wallets will soon integrate with aggregated systems like Siri, Alexa, and Cortana. "Apps will soon be obsolete and replaced by these aggregation platforms," says Tor Opedal, vice president of North America QSR for **Mastercard**. He adds that quick serves need to properly train all employees involved with new digital ordering and payments platforms, as a bad consumer experience can severely hamper a brand. "Perhaps soon, consumers will be more loyal to an aggregation platform than to a brand," he says, "and a brand giving a bad consumer experience on these platforms can quickly be replaced by a consumer."

For now, mobile payments haven't gone mainstream in the quick-serve industry, and digital wallet providers are aware that they must bring more value to the consumer to start seeing higher adoption rates. Castrechini predicts a significant investment from many parties in the payment ecosystem this year. Her advice to restaurateurs: "The best way to prepare for these disruptive technologies is to think through the best possible experiences for customers. Then work closely with solution and payment technology providers to determine the best solution to get you to those experiences." SC