

NAVIGATING THE PAYMENTS AND SECURITY LANDSCAPE

Payment disruptions impacting
restaurant owners today



Almost every month we hear a news story about another data breach that compromises the security of payment card data for thousands, and sometimes millions, of cardholders. Fraudulent payment card schemes not only disrupt the lives of consumers, the schemes also affect the trust and financial liability of the businesses who accept those cards.

The payment card security landscape is quickly changing due to more sophisticated fraud methods and emerging technologies to prevent these threats. We can help you navigate through all the considerations and determine the best payment solutions to secure your business.

Three payments and security trends are causing disruptions for restaurant owners:

- Increasing need to protect the business from data security threats
- Upcoming shift in liability for fraudulent card charges (EMV)
- Growing emergence of mobile wallets

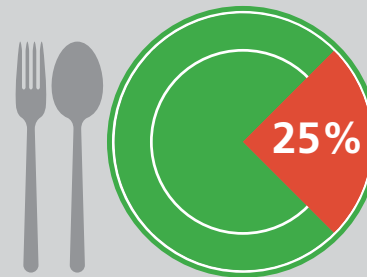
- | | | | |
|---|--|---|---|
| 1 | Data Security Threats: Think they can't happen to you? | 4 | What does EMV mean for your business? |
| 2 | Data security breaches cost you and your customers | 5 | Accepting EMV payments impacts everyone |
| 3 | So how can you ensure every payment is secure? | 6 | Everyone is talking about mobile wallets...are you? |



Data Security Threats: Think they can't happen to you?

You may think that your restaurant is too small to be of interest to cyber thieves. This kind of thinking can promote a false sense of security. According to a 2015 Trustwave report, 97 million card numbers were stolen last year and **25% of all data security breaches occurred in the hospitality/food and beverage space.**

97 million
card numbers were
stolen last year.



of all data security
breaches occurred in
the hospitality/food
and beverage space.



Data security breaches cost you and your customers

Consumers expect you to protect their financial data. In a poll of American shoppers, 88 percent of the 1,060 people surveyed place the burden of protecting the data on the businesses that collect it.¹ Consumers who use their payment cards at your restaurant place a high level of trust in your systems, and that trust can be broken with just one security breach.

A global survey released in May 2015 conducted by Ponemon and sponsored by IBM reported on the increased cost of data breaches to retailers and enterprises. The

survey found that the cost of a data breach increased to \$217 per person in 2015 from \$201 in 2014. This number includes direct costs such as credit monitoring services and legal fees as well as indirect costs such as customer turnover, increased customer-acquisition activities and diminished goodwill.

Depending on the number of transactions you process each year, **the total cost of a data security breach could potentially exceed \$1 million.** Most importantly, the damage to your brand's reputation may take years to overcome.



88% of American shoppers surveyed place the burden of protecting the data on the businesses that collect it.

Source: 1. Associated Press – GfK poll of American consumers, January 17, 2014



So how can you ensure every payment is secure?

Everyone agrees that increasing the security of cardholder data is top priority. But it can be hard to know how to best protect your business. **One solution is point-to-point encryption (P2PE)**, a broader layer of security for the payment transaction. P2PE ensures that all cardholder data is fully protected within the payment terminal device and 'in flight' to the processing center. Data is encrypted at the point-of-swipe and only decrypted after it arrives safely at electronic payment datacenters.

How is this an effective way to secure card data? A criminal who hacks into a merchant's network that has implemented P2PE could not easily use the encrypted credit card data to produce fraudulent cards. The responsibilities of PCI DSS compliance remain even when implementing P2PE; however, point-to-point encryption significantly reduces the risk of a security breach in the form of card data being intercepted on its way to the payment processor.





What does EMV mean for your business?

Credit card companies are enacting their own measures to combat fraudulent card processing activity by producing cards with **new chip-based technology to read card data**. The technical standard for this technology is called EMV (Europay, Mastercard, Visa). Its purpose is to curtail criminal activity by verifying that a credit card is authentic at the time of purchase.

The new chip cards contain an embedded microchip that authenticates each transaction by sending a unique code from the card to the card issuer via a merchant terminal. Once the issuer confirms the card's authenticity, the transaction goes through. Transactions will take a few seconds longer, but they will be more secure.

Additionally, credit card companies are shifting liability for fraudulent charges. Starting October 1, 2015, if your business accepts and processes a fraudulent transaction on a non-smart-chip/EMV enabled terminal, the liability for that transaction lies with the entity that is least EMV-compliant.

For small business owners, **EMV is a risk decision, not a regulatory one**. While October 1, 2015 is a real date for the liability shift, merchants who do not switch over to EMV will not be fined and will still be able to accept magnetic stripe credit cards.

Since the adoption of EMV chip-and-pin technology in the UK in 2003, **counterfeit fraud in the UK has reduced by 70%**, according to a 2015 Barclays report.



EMV Myths Debunked

Still have questions about EMV regulations? Check out our [EMV Myths Debunked blog](#) to get the truth about the payment security technology and the potential liability for your restaurant.



Myth: Implementing EMV in your business is required and will be enforced by a government regulation or security council.

Reality: EMV is not mandated or regulated by a government body or council. Presently, no one can threaten you with a fine for not implementing EMV-enabled payment devices by October 1.



Myth: EMV is a requirement for complying with PCI Data Security Standards.

Reality: While EMV is one component to building an overarching, cohesive data security strategy that helps you reduce your liability risk, implementing EMV is not a requirement to achieve PCI compliance.



Myth: Once you implement EMV, you will no longer be able to accept credit cards with magnetic stripes.

Reality: Credit cards with magnetic stripes will be in circulation for quite some time – even newly issued EMV cards will have magnetic stripes to allow for payment at businesses that have not yet implemented EMV.



Myth: EMV protects your business from a data security breach.

Reality: While EMV can help safeguard against fraudulent purchases, it does not protect a business from any malicious network attacks or data security breaches.



EMV Myths Debunked



Myth: EMV will rapidly achieve mass adoption by both credit card issuers and other businesses.

Reality: The U.S. transition to EMV is going to be gradual and is expected to continue well after the October 1, 2015 liability shift date.



Myth: Transitioning to EMV is as simple as plugging in a new payment terminal

Reality: There are many complexities associated with the transition to EMV. In addition to EMV certifications needed for processors, payment terminal devices and point-of-sale software versions, there are also operational considerations that should be addressed before implementing EMV.



Myth: You do not need to worry about PCI Data Security Requirements if you use EMV.

Reality: Although EMV utilizes technology that improves the security of processing credit card transactions, it does not remove your requirement to comply with the Payment Card Industry Data Security Standard in order to protect your entire payment network.



Accepting EMV payments impacts everyone

To accept EMV transactions, businesses will need to implement payment devices that can process the new chip-card technology. But implementing this technology is more complex than just plugging in a new payment device or updating software. Instead, transitioning your restaurant to EMV involves many complexities.

Each component in your payment ecosystem has to undergo vigorous testing and certification processes to ensure they meet EMV specifications. This means that your POS system, your payment processor and the type of payment terminal device you want to implement all must be EMV-certified in order for your restaurant to begin taking chip card payments.

Additionally, **the transaction process itself will change**. Instead of swiping a credit card through a magnetic stripe reader on a POS system, the new chip-enabled credit cards will need to be inserted, or “dipped”, into an EMV payment terminal and remain there for 10-15 seconds for the duration of the entire transaction. Initially, this slower process may cause some confusion for guests and potentially impact your speed-of-service; it’s important that you train your staff on the differences with chip-card acceptance in advance of implementing EMV.





Training your staff on EMV

Your staff will need to know how to:



Recognize

the difference between chip and magnetic stripe cards



Insert

or 'dip' the EMV chip card and hold the card in the terminal until the transaction is complete



Educate

customers on how to use their new chip cards at the counter or the table



Understand

that each chip card transaction will take a few extra seconds to process



Inform

customers that the tip must be included before the transaction is processed



Remind

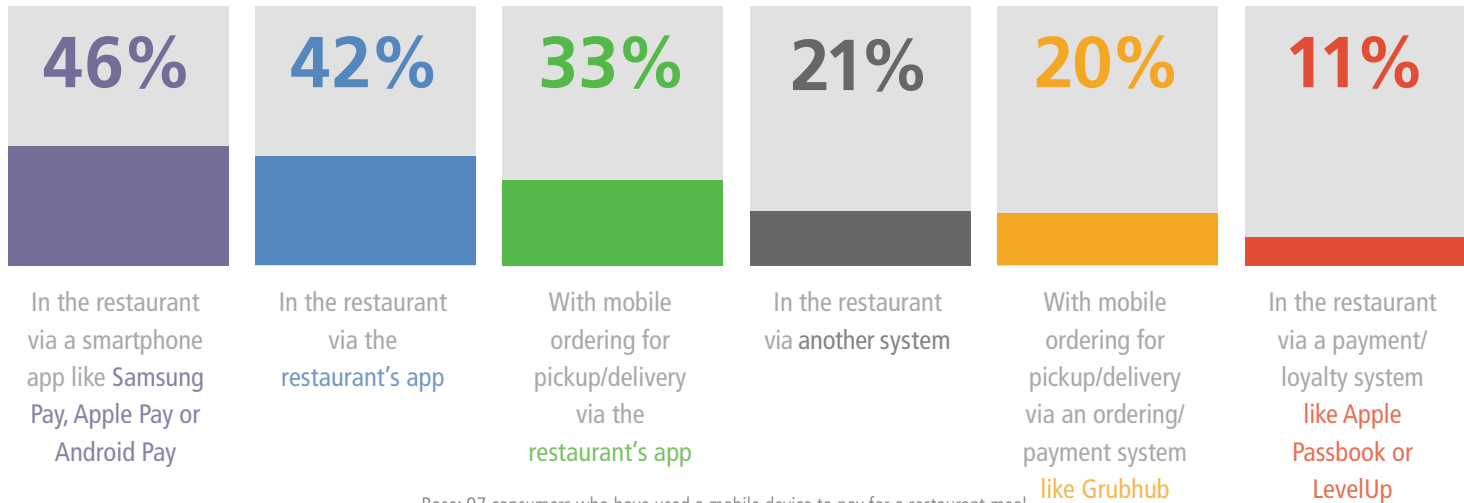
customers not to forget their credit card in the terminal



Everyone is talking about mobile wallets...are you?

The few extra seconds that it takes for credit card transactions to process using EMV technology may exasperate some consumers who are used to faster processing times. Some restaurant owners are looking beyond EMV and investing in accommodating mobile wallet providers like Apple Pay, Android Pay and Samsung Pay. **Mobile payments are expected to grow to \$34 billion** in transactions in 2019, up from \$8 billion in 2015. Players, technology and suppliers are changing so rapidly that it is easy to get overwhelmed.

Under what circumstances have you used mobile payment?



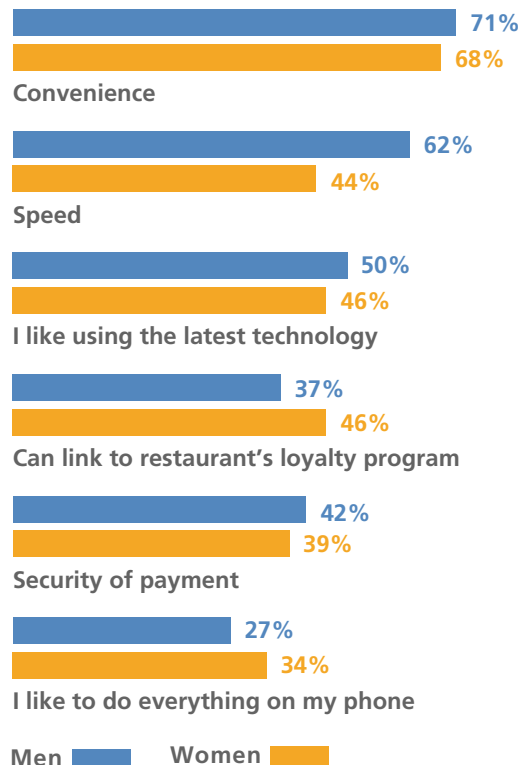
Base: 97 consumers who have used a mobile device to pay for a restaurant meal
Technomic Inc., January 2015



Customers say they want the flexibility to pay when they are ready and the option to pay with their mobile device. Restaurants may want to add these new payment options, but they don't want the disruption and added cost that may accompany them. Most importantly, any new payment method should be evaluated in the context of an overall strategy that emphasizes security. Here are a few items to consider when addressing mobile payment options:

- 1 Mobile payment methods can speed up the line and improve the customer experience.
- 2 Any mobile payment solution will need to integrate with your current POS system.
- 3 Many mobile payment solutions, such as Apple Pay or Android Pay, utilize tokenization as part of their solution. Tokenization can improve security by replacing sensitive data with unique identification symbols that retain essential information without compromising its security through the payment network.

What did you like about paying for your meal by mobile phone?



Base: 93 consumers (52 men 41 women) who have used a mobile device to pay for a restaurant meal and would likely do so again
Technomic Inc., January 2015

You can address these issues without disrupting your business.

Attract new customers and create an amazing experience that turns them into regulars.

Giving your guests a choice of payment options, along with securing their personal data, can build that loyalty. If you don't **have a payment security strategy in place**, however, it can be difficult to determine the right ways to move forward. NCR can help you develop a secure, compliance and mobile payment strategy that meets your needs today and prepares you for tomorrow.

For more information, please visit
www.ncr.com/hospitality,
call us at 1-877-794-7237
or email hospitality.information@ncr.com.

Contact us



Why NCR?

NCR Corporation (NYSE: NCR) is the global leader in consumer transaction technologies, turning everyday interactions with businesses into exceptional experiences. With its software, hardware, and portfolio of services, NCR enables more than 550 million transactions daily across retail, financial, travel, hospitality, telecom and technology, and small business. NCR solutions run the everyday transactions that make your life easier.

NCR is headquartered in Duluth, Georgia with over 30,000 employees and does business in 180 countries. NCR is a trademark of NCR Corporation in the United States and other countries. The company encourages investors to visit its web site which is updated regularly with financial and other important information about NCR.

NCR Corporation | 3097 Satellite Boulevard . Duluth, Georgia 30096 . USA

NCR continually improves products as new technologies and components become available. NCR, therefore, reserves the right to change specifications without prior notice. All features, functions and operations described herein may not be marketed by NCR in all parts of the world. Consult your NCR representative or NCR office for the latest information. All brand and product names appearing in this document are trademarks, registered trademarks or service marks of their respective holders.

©2015 NCR Corporation Project# 15HOSP3502-0715 www.ncr.com

