Preparing Your Business for EMV Payments

An Essential Guide to Protecting Your Sales, Profits and Brand

Beginning October 1, changes in credit and debit card processing standards shift certain liabilities to businesses with outdated processing terminals. This guide shows you what you need to understand and prepare for EMV, strengthen your data security standards, protect yourself from chargeback liability, and realize all the marketing advantages that EMV migration offers for your business.

Brought to you by

Entrepreneur

sage

EMV chip debit and credit card technology is already the standard in most of the world, and it's finally being introduced on a large scale here in the U.S. That's good news for small-business owners and their customers, because the new cards' technology enhances security.

Deploying EMV technology has already played an important role in combating credit card fraud in markets abroad. Replicating that success in the U.S. requires us to transition to the use of these new cards and the next-generation processing terminals compatible with the chip technology's security enhancements.

Known as the EMV migration ("EMV" stands for Europay, MasterCard, and Visa, the three companies behind the new global standard for credit and debit card acceptance), this transition offers a variety of opportunities for your business when you install and activate the new terminals. In an era of frequent news reports about customer data breaches, they give you a tangible, visible means of demonstrating your concern for data security.

This has been shown to increase customer confidence and loyalty, which in turn improves your ability to grow sales. In addition, deploying EMV-capable terminals helps you gain the ability to accept emerging forms of mobile payment, which may help you capture a greater share of the growing millennial market—the customers of the future.

Most of all, adoption of EMV chip-compatible payment terminals protects you and your customers from credit and debit card fraud. The security impact of EMV chip card technology is so significant that the major credit card brands have set October 2015 as the launch of an important liability shift. From that date forward, businesses that don't have equipment able to process EMV-enabled debit and credit cards will be financially liable for chargebacks that stem from counterfeit fraud.

This guide provides information about what you need to do to install and activate the new terminals, strengthen your data security standards, protect yourself from chargeback liability, and realize all the marketing advantages that EMV migration offers for your business.

The Need for New Fraud-Fighting Measures

To fully appreciate the value of this opportunity to get ahead of payment changes on the horizon, it's helpful to understand the magnitude of the current data security problem and the burden it places on small businesses in the U.S.

The U.S. is experiencing counterfeit credit card fraud at a much higher rate than the rest of the world. In October 2014, a study released by the Nilson Report showed that worldwide, card fraud losses totaled $11.3 billion in 2012, a 14.6 percent increase over the previous year. In the U.S. alone, however, card issuers and businesses lost $3.4 billion and $1.9 billion, respectively. That's 47 percent of all the fraud that occurred globally.

The size of this market skews those figures to some extent, and so does the volume and growth of credit and debit card use here, as the Nilson Report acknowledged. It found that purchases made by customers using the four major credit and debit card brands rose 8.9 percent from 2013 to 2014, when they accounted for $4.442 trillion in spending at U.S. businesses. "Fraud losses on all general purpose and private label, signature and PIN payment cards reached $5.33 billion in the U.S. last year, up 14.5 percent," the report noted.

While the use of cards is surging in this country, our card technology lags behind that of much of the world, where microchip-enabled cards have largely replaced the magnetic-strip-only cards still prevalent in the U.S. Cards equipped only with magnetic stripes are the low-hanging fruit in terms of fraud opportunities for transactions processed at terminals.

The EMV migration and the coming liability shift are a response to these facts and a means of making terminals tools for preventing, rather than enabling, credit and debit card fraud. With an increasing number of issuers putting chip-enabled cards in consumers' hands, the time is right for small businesses to upgrade to EMV-compatible payment terminals.

While keeping up with global standards is part of the issue, you should also consider the potential brand protection EMV migration offers. "Any company that suffers a breach has a reputational hit that is every bit as costly as the specific dollar amount associated with that breach," says Rob Bertke, senior vice president of Research and Development at Sage Payment Solutions.

Business owners who opt out of EMV migration will be held liable for fraudulent purchases made on outdated terminals.

"No company wants that to happen; no company wants their brand damaged in that way. Fraudsters are smart. They're clever. And they're always going after the weakest link. So our advice is please, please, don't be the weakest link. Don't look at this as just an arbitrary cost. Look at it as a value to protect you and your business. You will reap benefits well beyond the cost of a piece of hardware that goes into your store."

Liability Protection for Small Businesses

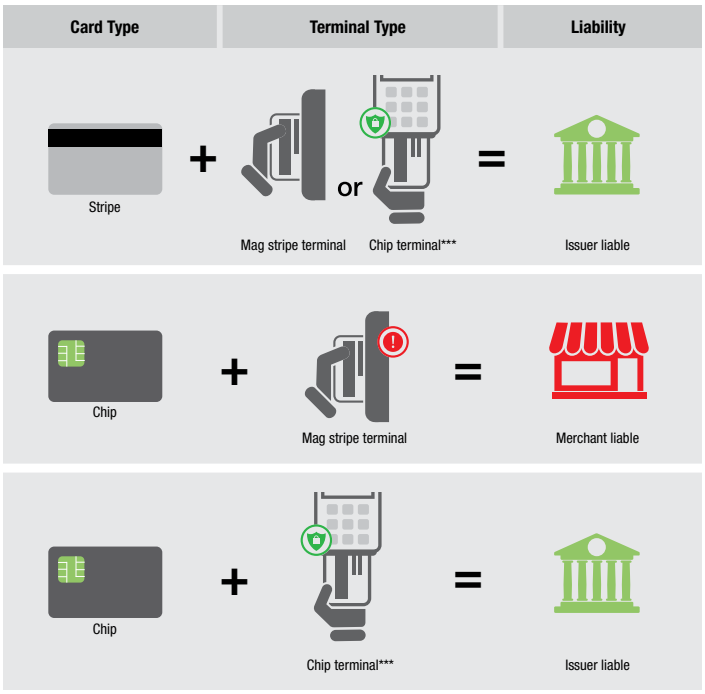
Cards that use chip technology will continue to be equipped with the magnetic stripes necessary to be used at older terminals, and the move to new terminals is voluntary: small-business owners face no legal requirement to upgrade. However, those who choose not to adopt EMV will be leaving themselves open to expensive repercussions.

"You do have a business choice, and obviously, every business wants to avoid costs," says Bertke. "But with any cost, you have to consider the value. Look at the amount of credit card fraud in the U.S. and the way card-present fraud has decreased in countries that have implemented EMV. You can quickly see that there's a real value in changing the way that we take credit cards."

There's no debating the connection between deploying new terminals and improving security. "The upgrade to chip creates a more secure transaction," says Carolyn Balfany, senior vice president of U.S. Product Delivery at MasterCard. "It makes it nearly impossible for fraudsters to counterfeit, and counterfeit fraud is the majority of the fraud that is seen here in the U.S."

Counterfeit Card Fraud Liability*

October 2015 and beyond**



*Same applies for all brands. **October 2017 for AFD. ***With or without PIN capabilities

Small businesses who opt out of the EMV migration are therefore also opting out of the protection that the chip technology delivers, a benefit that extends to their customers as well as to business owners themselves. That's why the major credit card brands are instituting the liability shift in cases where fraudulent purchases made on the outdated terminals could have been prevented had the merchant adopted the new terminals. Conversely, upgrading to new terminals reduces the risk of (and the expenses related to) fraud and liability.

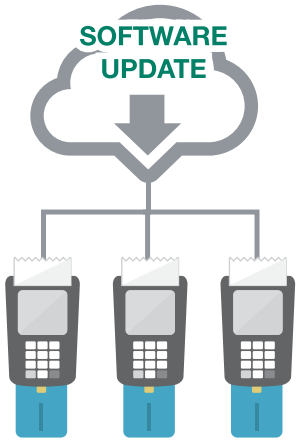
There are also EMV conversion solutions designed for tablets, so if your business processes payments on them rather than via terminals, you can also be covered by these improvements in security and fraud protection. The liability shift will apply to both types of devices as of October.

The Conversion Process: Hardware and Software

Small-business owners don't need advanced knowledge of technology to select EMV terminals and software. To get started, contact your merchant services provider to find turnkey solutions. They're there to help you understand the options available to your business.

"This doesn't have to be a big problem that you're going to need to expend lots of money and lots of time and effort on, as long as you plan in advance and communicate with your suppliers and financial payment processing partners," says Randy Vanderhoof, executive director of the Smart Card Alliance and director of the EMV Migration Forum. "Doing that sooner rather than later is going to be better. The closer you get to the October timeline for the liability shift, the more difficult it's going to be to get the same level of support and service from financial institutions and processing partners, because they're going to be scrambling to keep up demand."

Merchant service providers are able to support small-business owners not only through the hardware purchase, but also in the implementation and activation of the solution, which involves downloading software to run the new terminals. In fact, small businesses who own newer terminals may find that they already have the hardware necessary to process an EMV card. In those cases, they'll just need a software update to become EMV-compliant.



"Just having the hardware is actually a smaller part of the EMV solution," says Allen Friedman, director of Payment Solutions at Ingenico North America/Ingenico Group and a Certified Smart Card Industry Professional. "The liability shift that is coming in October requires that you be able to process EMV cards, which requires you to have not just the hardware, but also the application to make use of that hardware."

Strategies for Making a Smooth Transition

The benefits to protecting your brand's reputation can far outweigh the cost of upgrading.

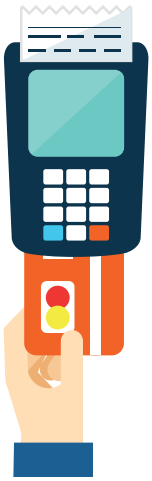
With so much support available, there's no need to be intimidated by the process of deploying new terminals. Adopting a methodical approach is the key to completing a successful transition. The costs of upgrading can be anywhere from zero to $500 per terminal, so experts advise asking about promotional offers or pricing structures that can help minimize the expense.

"Individual business owners should feel empowered and know that there's information out there for them," Balfany says. "Small businesses should really engage their payment processors. They're really quite capable now of talking to them about their options."

Several of those options allow you to complete the conversion in stages, Vanderhoof notes. You can, for example, convert one store or one register terminal at a time to make a test run before upgrading devices company-wide. Other businesses have already installed EMV-capable terminals but deferred activating them for use with chip cards. "Those terminals will continue to process payment transactions with magnetic stripe cards for as long as the merchant deems necessary before they activate them or enable them to start accepting chips," he says.

Once the new hardware and software is installed, the remainder of the learning curve involves simply getting used to the new way cards and terminals interact. Unlike magnetic stripe cards that are swiped, chip cards are inserted into a slot in the terminal. What's more, chip technology is smart enough to prevent the new cards from being used incorrectly.

A consumer who, by force of habit, automatically swipes a chip card at an EMV-capable terminal will be given a prompt to insert the card into the chip slot. The new terminals are programmed to prevent use of the magnetic stripe and to complete transactions only when the card is used correctly, which helps ensure that both the consumer and your business realize all the benefits of EMV. You should be prepared to train your staff in the use of the new terminals and assist customers as they get used to the new process, which will quickly become familiar to everyone.



"It's really just a matter of getting through those initial stumbles that are going to happen for first-time shoppers that they're going to have to deal with," Vanderhoof says. "But as more and more businesses start enabling in the next few months, there's going to be more and more likelihood that customers will already have experienced a payment transaction somewhere else with a chip. That will reduce the number of failed attempts pretty rapidly." In the interim, assisting customers helps them see that your business cares about their security.

Added Benefits: Keeping Pace With New Customer Payment Preferences

In addition to minimizing liability and protecting your brand reputation, adapting to EMV demonstrates the kind of leading-edge thinking customers appreciate. That's because the EMV migration isn't the only change on the horizon: there's also growing consumer interest in and use of contactless systems such as Google Wallet, Apple Pay, and Android Pay, particularly among millennials.

"Merchants are expected to adapt to the way consumers want to pay," Balfany says. "So a lot of small businesses are taking this opportunity to upgrade their terminals not just to accept contact chip cards, but also to accept contactless payments. I really encourage small businesses to look at the ability to facilitate more payments as they do the upgrade."

Just as you can create a competitive distinction by implementing EMV in advance of the October liability shift, you can also make a strong impression for your business as an early adopter of these mobile payment platforms. "Look at EMV as a change agent and think about the way you can leverage that," Bertke says. "That simple move, whereas it might feel costly, is actually changing the entire way you interact with your customer and can ensure that you get the most spend out of your customers."

By making these changes, you can demonstrate your company's dedication to safeguarding customer financial data and its commitment to innovation. These positive associations can translate to increased customer confidence, sales and growth.

EMV Resource Guide

Looking for more information about what the EMV migration involves and what you need to do to get ready? Visit **Sage's EMV website** which offers guidance for small to medium-size businesses on preparation along with an EMV FAQ and information about terminals.

In addition, these online resources can help you create a blueprint for making optimal use of the protections available to your business and your customers.

The **EMV Connection website** developed by the non-profit, multi-industry Smart Card Alliance, features a merchant page designed to assist business owners with the full spectrum of EMV migration matters, "from EMV basics to detailed guidance on what merchants need to consider to develop the roadmap to accept EMV cards and devices."

GoChipCard.com was created by the EMV Migration Forum and the Payments Security Task Force "to assist consumers, merchants and issuers with the migration to chip technology." The merchant section of the site offers training FAQs, a training infographic, and a guide to communication best practices. To access these resources, scroll to the links found beneath the label "Merchant Resources" found at the bottom of the page.

The **MasterCardBiz blog** includes an "EMV Central" section that offers a variety of resources designed to help small merchants understand the EMV migration and prepare for its implementation in their businesses, including:

- **A Short Video, MasterCard EMV 101 for the Small Merchant**
- **An EMV FAQ**
- **The DL on Chip Cards Infographic**

Visa created this infographic with accompanying text that explains what an EMV chip card is and how it works.

Additional Security Resources

These additional resources can help you ensure your business is compliant with existing security standards.

The **Federal Communications Commission's 10 Cybersecurity Tips for Small Business** shows owners of small companies how to "protect themselves, their customers, and their data."

The National Cyber Security Alliance created its **StaySafeOnline resource** to offer guidance on protecting "your business, employees, and customers from online attacks, data loss, and other threats."

Launched in 2006, the PCI (Payment Card Industry) Security Standards Council develops, manages, and provides education on and awareness of the PCI Security Standards. Those standards were created to meet these objectives: "build and maintain a secure network; protect cardholder data; ensure the maintenance of vulnerability management programs; implement strong access control measures; regularly monitor and test networks; and ensure the maintenance of information security policies." Visit its website to access these resources, which were created to meet the needs of small-business merchants:

- **PCI for Small Merchants**
- **Secure Passwords**
- **Protecting Your Customer's Data from Malware**
- **Top 10 Tips for Protecting against Card Fraud**

sage Your Payment Solutions Partner

Established more than 30 years ago, Sage provides small and medium sized organizations and mid-market companies with a range of easy-to-use, secure and efficient business management software and services—from accounting, HR and payroll, to payments, enterprise resource planning and customer relationship management.

For more information about how we can work together to meet your EMV migration needs and support your business objectives, visit **sagepaymentsemv.com** or call us at **800-652-2370**.