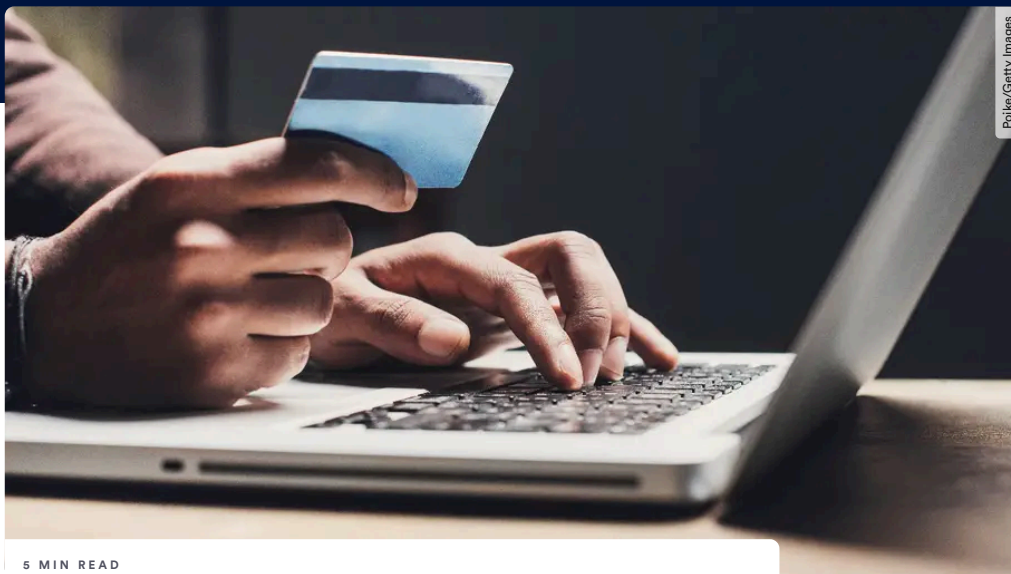


CREDIT CARDS > BUSINESS

[Advertiser Disclosure](#)

What is EMV compliance law and should your business worry about it?

SHARE:    

5 MIN READ

December 06, 2023

Written by **Holly D. Johnson** and **Poonkulali Thangavelu**Edited by **Sarah Gage**

The Bankrate promise

[More info](#)

At Bankrate we strive to help you make smarter financial decisions. While we adhere to strict [editorial integrity](#), this post may contain references to products from our partners. Here's an explanation for [how we make money](#). The content on this page is accurate as of the posting date; however, some of the offers mentioned may have expired. Terms apply to the offers listed on this page. Any opinions, analyses, reviews or recommendations expressed in this article are those of the author's alone, and have not been reviewed, approved or otherwise endorsed by any card issuer.

Key takeaways

- Businesses should be EMV compliant to avoid being held responsible for credit card fraud.
- EMV compliance requires businesses to use EMV card readers to process credit card transactions.
- Your business could still face liability for fraud in some situations, even if you are EMV compliant.

As with all forms of payment, using a credit card comes with an inherent level of risk. After all, hackers and thieves make a career of figuring out ways to steal your credit card details so they can run up fraudulent charges. This is true for in-person purchases, as well as those made online.

Fortunately, many [credit cards come with zero fraud liability](#) protection, meaning you won't be on the hook for fraudulent charges posted to your account. Further protection afforded by the Fair Credit Billing

Chip card protections

Another layer of protection you can expect to see with most credit cards comes in the form of a chip. [Chip-enabled credit cards](#) are also called EMV-enabled credit cards, due to the EMV technology used to create them (EMV stands for “Europay, Mastercard and Visa,” signifying the three major credit card providers).

Before chip technology, all credit cards used a magnetic stripe to store cardholder data. But where magnetic stripe credit cards can be “[skimmed](#)” by hackers and thieves, this type of theft is much less common with chip credit cards.

Today, chip cards can be either:

- Chip and PIN cards, which require customers to enter their personal identification number (PIN) to complete a transaction, or
- Chip and signature cards, which use a signature instead of a PIN to verify the cardholder’s identity.

With both types of chip cards, the embedded chip holds your payment data and provides a unique code for every purchase you make. The code that is generated is only good for that single transaction, and the codes are always changing. As a result, credit cards with chip technology are considerably more difficult to hack than their magnetic stripe counterparts.

While EMV technology is intended to cut down on consumer credit card fraud, it also helps businesses reduce [chargebacks](#) that result from fraudulent purchases.

How do I use an EMV card to make a purchase?

Compared to swiping magnetic stripe cards, completing an in-person transaction with an EMV-enabled credit card requires a different process.

Specifically, both chip and PIN and chip and signature credit cards require shoppers to dip their credit card into the terminal, at which point the card is read and a unique token is created for the transaction. From there, cardholders either enter their PINs (if they have chip and PIN credit cards) or provide their signatures (if they hold chip and signature cards).

What is the EMV compliance standard?

Major credit card issuers asked that most U.S. businesses that accept credit cards move toward an EMV-compliant credit card point of sale (POS) system by Oct. 1, 2015 (for fuel retailers, the EMV liability deadline was April 2021).

fraud. After this date, however, liability shifted to whichever party — the merchant or the card issuer — was the least compliant with EMV requirements.

In theory, this deadline should have been enough to motivate businesses to change their payment systems in order to reduce fraud and avoid financial losses. However, many businesses have not yet upgraded their payment systems, though there is momentum in the right direction.

According to [Visa](#), the number of U.S. retailers who accept EMV-enabled cards increased 825 percent from September of 2015 until June of 2019, growing from 392,000 to 3.7 million merchants.

How does EMV compliance affect you as a business owner?

Businesses are not currently being fined for not upgrading their payment systems. If you're a business owner who hasn't yet upgraded to EMV-compliant systems, you should do so — but you won't be on the hook for government penalties if you don't make the change.

While EMV compliance is more of an industry standard that serves as a guideline, rather than a government-mandated law, you could still face liability for fraud and chargeback situations if you aren't compliant.

When will you be liable?

If you haven't upgraded to an EMV-compliant card terminal, but you process EMV credit card transactions, you may be found liable if any fraud occurs. That's because, although the card issuer was compliant, you aren't since you haven't upgraded your card reader to be EMV compliant.

Even if you have upgraded to an EMV-compliant card terminal, you may be liable for fraudulent transactions if you manually entered the customer's card information, rather than processing the card in the terminal.

When will you not be liable?

If you process a magnetic stripe card on your EMV-compliant card terminal, and the transaction turns out to be fraudulent, you likely won't be held liable since you used an upgraded card reader.

Further, if you process an EMV credit card on your EMV-compliant system, and the transaction turns out to be fraudulent, you shouldn't be held responsible since you're compliant with the EMV standard.

How small businesses should adjust their practices

In order to minimize your risk of being held liable for credit card fraud, there are a few measures you'll want to take. To start, ensure you're compliant with the EMV standard, and make the switch to an EMV-

Also, make it a practice to keep copies of credit card receipts and relevant order documentation. If you ever have to make a case to a card issuer refuting a customer chargeback, having all the information at hand can help you make a good case. For instance, in a case of “card not present” fraud, you could present the issuer with shipping information and delivery confirmation, as well as any records of your communication with the customer.

Finally, make it a policy that, if a customer transaction doesn’t go through on your EMV-compliant card reader, you won’t [manually enter their card information](#).

The bottom line

EMV-enabled credit cards are usable anywhere credit cards are accepted, but you should also know [the U.S. is somewhat behind](#) when it comes to EMV technology. In Europe, for example, most countries made the transition to EMV technology years ago, and chip and PIN cards are now the norm.

If you’re a business owner, be aware that, while you can’t be legally prosecuted for not upgrading to EMV-compliant payment systems, making the switch should still be a priority. With the deadline for EMV implementations now past, you risk facing liability in credit card fraud situations if your business remains out of compliance with this industry standard.



Written by

Holly D. Johnson

Author, Award-Winning Writer

✕ ⓘ

[Read more from Holly](#)

Holly Johnson writes expert content on personal finance, credit cards, loyalty and insurance topics. In addition to writing for Bankrate and CreditCards.com, Johnson does ongoing work for clients that include CNN, Forbes Advisor, LendingTree, Time Magazine and more.



Co-written by

Poonkulali Thangavelu

Former Senior Writer, Credit cards

✕ ⓘ ✉

[Read more from Poonkulali](#)

Poonkulali Thangavelu is a senior writer and columnist at CreditCards.com and Bankrate, addressing debt and credit card-related legal and regulatory issues.



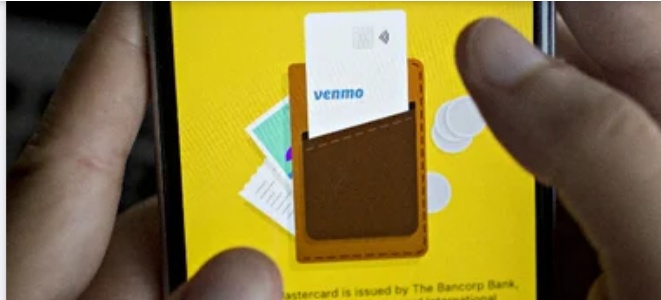
Edited by

Sarah Gage

Senior Editor, Credit Cards

Related Articles

ON THIS PAGE



REVIEWS

The Venmo Debit Card: Is it right for you?

6 MIN READ

Jun 04, 2024



ADVICE

How major credit card networks protect customers against fraud

6 MIN READ

Apr 24, 2023



ADVICE

RFID credit cards: Should you worry about protection?

4 MIN READ

Dec 17, 2021



ADVICE

Should a business notify me about a compromised credit card?

3 MIN READ

Nov 22, 2021

Bankrate

About

[About us](#)[Press room](#)[Careers](#)[Advertise with us](#)[Site map](#)

Legal

[Privacy policy](#)

Help

[Contact us](#)[Compare rates](#)[Latest news](#)[Popular topics](#)

ON THIS PAGE



Do not sell or share my personal information

Consumer Health Information Privacy Policy

Understanding Bankrate's averages

Terms of use

GLBA annual notice

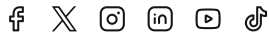
California Consumer Financial Privacy Notice

Licenses

How we make money

Bankrate.com is an independent, advertising-supported publisher and comparison service. We are compensated in exchange for placement of sponsored products and services, or by you clicking on certain links posted on our site. Therefore, this compensation may impact how, where and in what order products appear within listing categories, except where prohibited by law for our mortgage, home equity and other home lending products. Other factors, such as our own proprietary website rules and whether a product is offered in your area or at your self-selected credit score range, can also impact how and where products appear on this site. While we strive to provide a wide range of offers, Bankrate does not include information about every financial or credit product or service.

Bankrate, LLC NMLS ID# 1427381 | NMLS Consumer Access
BR Tech Services, Inc. NMLS ID #1743443 | NMLS Consumer Access



© 2024 Bankrate, LLC. A Red Ventures company. All Rights Reserved.