A Merchant's Guide to Simplified PCI Compliance.

PCI Plus is the easy, low-cost program for becoming and remaining PCI DSS compliant.



NorthAmerican BANCARD | PCI Plus | PCI DSS COMPLIANT

Table of contents.

The situation....3
The rise of fraudsters....4
The rise of PCI compliance....5
What is PCI compliance....6-7
Notable data breaches....8
The threat to small businesses....9
The importance of being compliant....10
PCI compliance classifications....11
The basics of compliance....12
The struggle to become and maintain compliance....13-17
PCI Plus....18
PCI Plus Tiers....19
No Tier....20
Tier I....21
Tier II....22
Tier III....23
Simplified PCI compliance....24
SecureTrust™....25
Low-fee and no-fee options....26
How to take advantage of PCI Plus....27
Contact us today....28


Your business is at risk.

Make no mistake ...

As the payments world gets more complex, so too, does the sophistication of fraudsters. Over the years, the threat of cardholder information becoming compromised has shifted from a copy of the swiped credit card receipt being stolen from your trash, to criminals actively:



Placing credit card skimmers on ATMs, at gas pumps, and within POS devices.



Installing malware or viruses on electronic devices.



Making attacks on company data repositories.

Examples of newer payment methods and services you may be offering that could be at risk of compromise:

- **Prepaid cards.**
- **Mobile payments.**
- **Ecommerce payments.**
- **Virtual currencies.**
- **Internet-based payment services.**

The rise of PCI compliance.

The good news is your business, regardless of size or industry, can easily protect your company and customer data right now. This is where PCI compliance comes in.

Unfortunately, given the complexity associated with staying compliant, most merchants (outside of large corporations with dedicated IT security personnel) do not maintain compliance because they lack the time and resources.

This is why we've introduced our PCI Plus program. We want to do everything we can to help our merchants achieve compliance and keep private cardholder data out of harm's way.



What exactly is PCI compliance?

Removing the mystery from PCI DSS.

PCI compliance, specifically PCI DSS (Payment Card Industry Data Security Standards), are a set of security requirements designed to ensure companies that process, store, and/or transmit credit card information maintain a secure environment.

The 1990s and early 2000s opened up new opportunities for merchants. Not only were they using electronic communication methods that didn't exist before, but they were also exploring new ways to expand revenue leveraging ecommerce. Unfortunately, this new opportunity for revenue also gave rise to cybercriminals. They began to craft more sophisticated ways to hack cardholder information stored in processing systems and payment networks.

The era of the data breach had begun.



Data breaches you may remember include...

2006

TJX (parent company of T.J. Maxx and Marshalls) — 94 million customer credit and debits cards are compromised.

2014

Home Depot — 56 million credit and debit cards are compromised during a malware attack.

2014

Capital One — The personal data of roughly 106 million customers and card applicants is stolen throughout the United States and Canada.

2016

Uber — 57 million riders and 600,000 drivers have their personal information compromised.

2017

Equifax — Personal info of 147.9 million consumers is exposed due to website vulnerability.

2019

Facebook — Approximately 540 million user records are compromised due to poor cybersecurity.

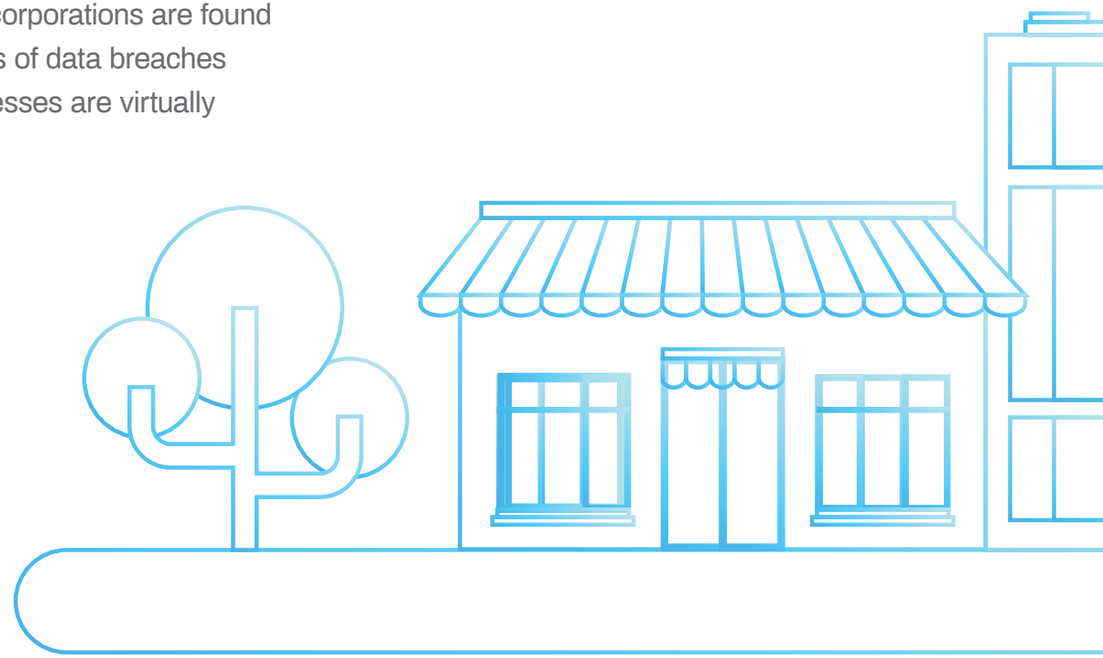
2019

First American — More than 885 million records are exposed including bank account info, SSNs, and international corporate documents.

Even small businesses are a major target.

While roughly 87 percent of small business owners believe they are not at risk of a data breach, it's simply not the case. The reality is, the very same data vulnerabilities that exist within large corporations are found in small businesses as well, and they are often even less protected. In fact, hundreds of data breaches happen each year to small businesses that we never hear about. Sadly, small businesses are virtually crippled when this happens.

The PCI compliance security requirements aim to eliminate those vulnerabilities.



VIEW ARTICLE

Why is becoming PCI compliant so important?

While damage to your reputation is one likely result of suffering a data breach, it's just the beginning. Failure to maintain PCI compliance could result in your business:

- **Losing customer trust.**
- **Being subjected to exorbitant non-compliance penalties.**
- **Being liable for a data breach done by cybercriminals!**

How is my business classified for PCI compliance?

The card brands have created different classifications of business when related to PCI compliance. The classification you belong to is based on your annual card transaction volume (credit, debit, and prepaid) and how you accept payments (in-store, online, or both).

LEVEL

1

Merchants processing **more than 6 million** transactions across all payment channels.

LEVEL

2

Merchants processing **1 to 6 million** transactions across all payment channels.

LEVEL

3

Merchants processing **20,000 to 1 million** online transactions annually.

LEVEL

4

Merchants processing **less than 20,000** online transactions annually, and all other merchants processing up to 1 million transactions annually.

The basic components of PCI compliance.

PCI compliance is acknowledged as the security standard for all businesses that store, process, and transmit cardholder data. Ensuring your business practices comply with the requirements institutes a fundamental level of security that helps reduce the likelihood of fraudulent activities and data breaches. While PCI compliance, in total, is quite complicated, there are three core elements of PCI compliance.



How your business handles card data

As the merchant, you are responsible for ensuring that sensitive card information is collected and transmitted in a secure manner, utilizing the latest in tokenization.



How your business stores cardholder data

It's equally as important to protect sensitive cardholder data that you store by using up-to-date encryption and running regular security tests against the access to card data.



Your annual validation of compliance

Regular validation helps to make sure the necessary security controls are in place, based on how your business is accepting payments. This validation is an essential key to making sure that data remains secure.

Did we mention there are 12 main requirements and 300 sub-requirements?

The reality is there's a lot that goes into becoming and remaining PCI compliant. The latest set of security standards has 12 main requirements with more than 300 sub-requirements. Do you have time to keep up with 300 sub-requirements? We're guessing it's unlikely.

On top of that, the PCI Security Standards Council revises the rules every three years, so saying that PCI compliance is complex is quite an understatement.





No wonder businesses struggle with PCI compliance!

PCI compliance guidelines aren't only meant for major retailers and large organizations. The rules apply to every business that relies on credit and debit cards for payment transactions, which is virtually every consumer-facing and many business-facing merchants in today's world. Despite that reality, it's true that the process of becoming and remaining PCI compliant is a struggle for many merchants. In fact …

According to a 2018 study, only 52% of merchants were compliant with PCI DSS regulations that year.

SOURCE

And, that figure is actually lower than the 55% of merchants who were compliant with PCI DSS regulations in 2017.

So why, as data breaches are increasing, is the percentage of PCI compliant merchants decreasing? The reality is that PCI compliance can be tough to navigate, especially if you are a smaller business with limited resources.

The complicated administrative process of becoming PCI compliant poses a significant obstacle for many merchants who are focused on growing their businesses and have no time to complete mountains of confusing paperwork or track every little thing going on inside their business operation.

Other obstacles to compliance.

Self-assessment questionnaires (SAQs)

These arduous questionnaires must be completed each year, yet time demands often supercede and this step is often forgotten, leaving a business at risk of being assessed non-compliance fees.

Lack of payment processor support

Instead of proactively working with you to help you become and remain PCI compliance, most processors simply impose fees at the end of each month penalizing you for non-compliance.

No PCI police

The reality is there is nobody going door to door or sending email alerts to make sure every business is compliant.

As you can see, PCI compliance is complicated business!
Luckily, PCI Plus is here to simplify things.

What is PCI Plus and how can it help me?

PCI Plus is North American Bancard's (NAB) program dedicated to simplifying PCI compliance for merchants just like you, while helping you avoid:

The hassle of time-consuming, annual compliance paperwork.

Becoming non-compliant — our team always has your back.

Costly non-compliance fees.

PCI Plus even offers qualified merchants up to $100,000 in reimbursement costs per MID in the event of a data breach!

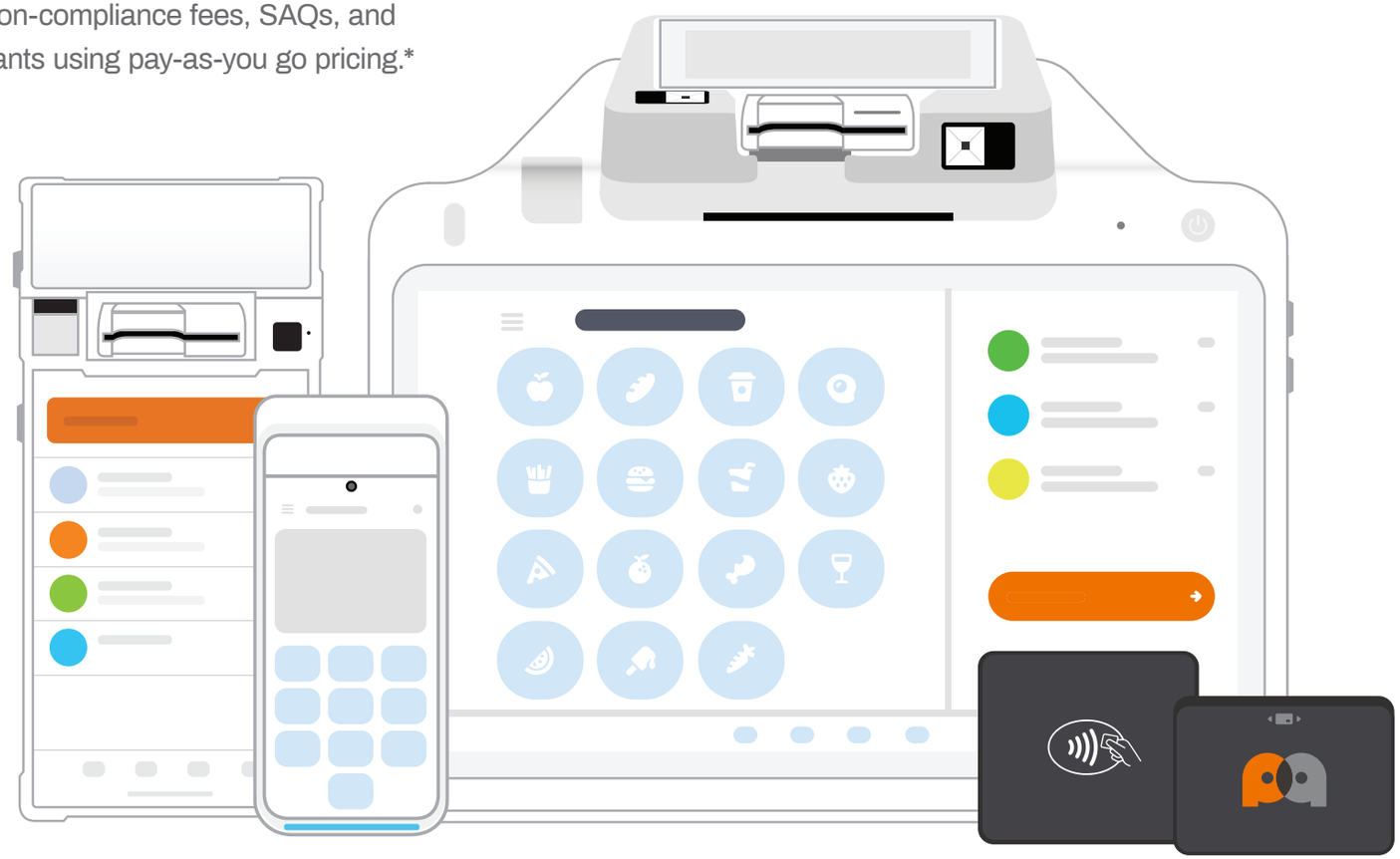
Multiple tier classifications/ billing options to choose from.

PCI Plus offers all merchants flexible billing choices for covering annual compliance fees upfront or monthly, as well as programs that exempt you from paying these fees altogether. Be sure to check with your Sales Partner or our PCI Plus compliance experts to confirm which tier and billing option best suits your business.

CONTACT US

No Tier.

This option, which eliminates program fees, non-compliance fees, SAQs, and scans, is available to all Payanywhere merchants using pay-as-you go pricing.*



*MID must have only Payanywhere to qualify. If additional equipment/solutions exist on MID, merchant may be subject to compliance requirements, including SAQs and scans.

Tier I.

$145
ANNUAL

OR

$12
PER MONTH

This option eliminates SAQs, scans, and non-compliance fees, and also includes breach forgiveness. Tier 1 includes all merchants using our Payanywhere Smart Solutions with custom pricing, boarded on Electronic Payment Exchange (EPX)*, our in-house payment processing platform. Merchants taking advantage of our Cash Discount or Flat-rate Pricing programs pay no fees at all.

*MID must have only Payanywhere to qualify. If additional equipment/solutions exist on MID, merchant may be subject to compliance requirements, including SAQs and scans.

Tier II.



This tier is available to:

- All EPX-boarded merchants using Verifone or Ingenico payment devices.*
  These merchants will not be required to perform SAQs or scans and also receive breach insurance.
- Compliant First Data and Global merchants.**
  These merchants will be required to perform SAQs and scans, if applicable, and also receive breach insurance.

Remember, merchants taking advantage of our Cash Discount or Flat-rate Pricing programs pay no fees at all.

*MID must have only EPX Verifone or Ingenico equipment to qualify. If additional equipment/solutions exist on MID, merchant may be subject to compliance requirements, including SAQs and scans. **These merchants may upgrade to EPX to avoid SAQ and scan requirements.

Tier III.



This tier, which requires SAQs and may require scans, covers non-compliant EPX merchants using payment devices other than Payanywhere, Verifone, and Ingenico. Non-compliant Global and First Data merchants also fall under Tier III.*

*Tier III merchants may become compliant and reduce their Tier III program fee and benefits to Tier II.

PCI compliance, simplified.

With PCI Plus, you'll always know:

- **How your business is classified.**
- **Whether or not you need to perform scans.**
- **Whether SAQs are needed.**

All while taking advantage of simplified billing that allows you to customize a solution to your specific business needs.

A compliance partner you can trust.

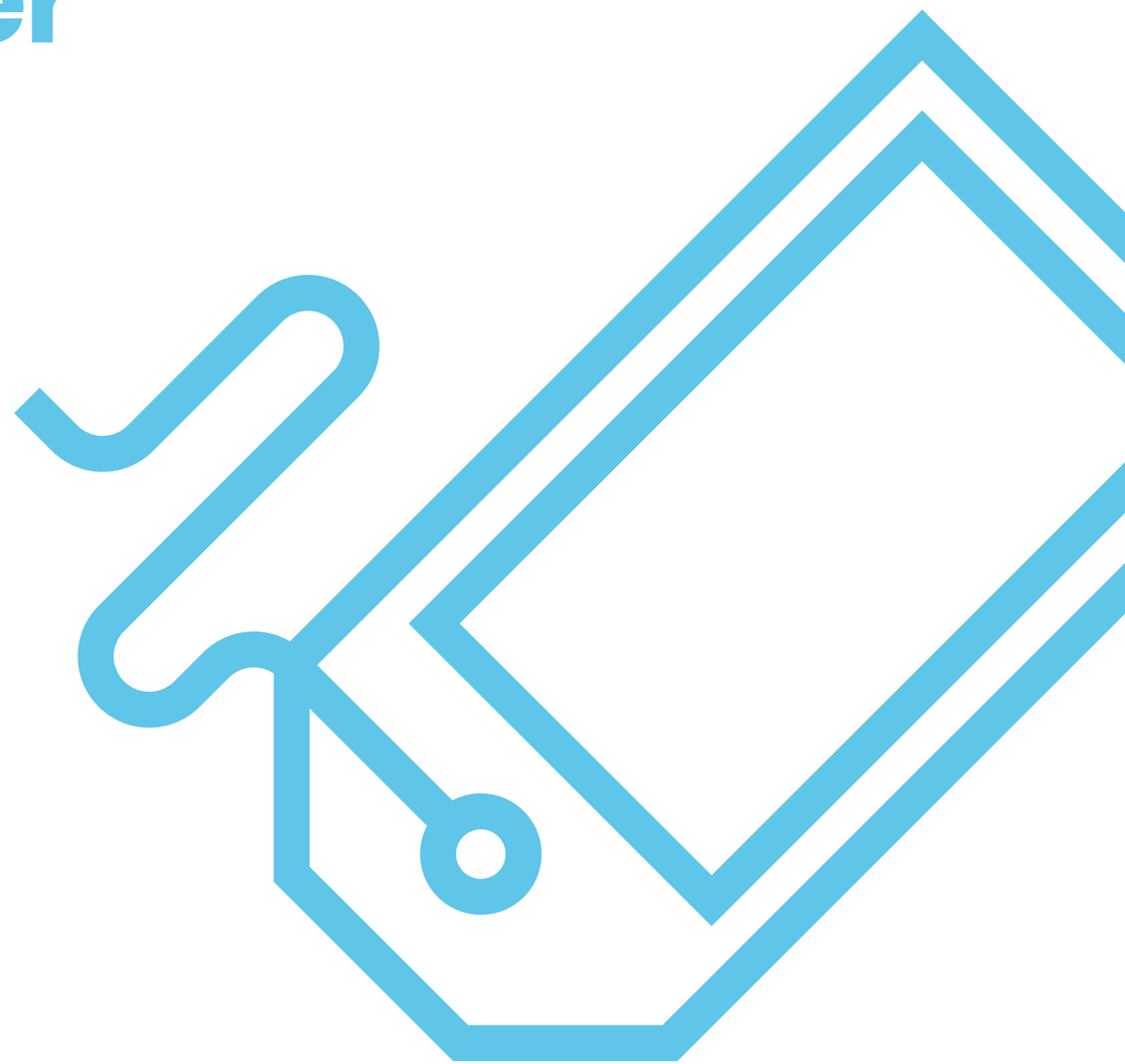
One of the best benefits of PCI Plus is it gives you access to SecureTrust™, an Approved Scanning Vendor (ASV) and Qualified Security Assessor (QSA). Our relationship with SecureTrust™ largely eliminates the need for our merchants to perform SAQs or scans!



Does PCI Plus offer low-fee options?

Yes!

By taking advantage of the upfront billing option, you're eligible for discounts and lower fees. Remember, you can even leverage NAB's Cash Discount and Flat-rate Pricing programs to eliminate program fees and non-compliance fees altogether!



How can I take advantage of PCI Plus?

Current Merchants
Non-compliant

It's easy! To confirm if your business is PCI compliant, look at your most recent statement. If you're paying a Tier III fee, then you are not currently PCI compliant. You can contact your Sales Partner directly, or call **855.613.7085**, to learn more about what steps you need to take to adjust your status.

Current Merchants
Good standing

If you're a former merchant in good standing, you've already been moved to the program.

New Merchants

If you partnered with NAB in December 2019 or later, you're already covered by PCI Plus!

If you aren't currently a merchant with us, but would like to be, please contact us at **cssales@nabancard.com**, or call **877.840.1952**, and we'll happily arrange time to speak with you about how you can take advantage of PCI Plus!

PCI Plus is the easy way to protect your customers and your business.

In today's era of cybercriminals, imagine being able to enjoy the peace of mind that comes with knowing an experienced team of PCI compliance experts will always be there to protect your business, so you can focus on growing it.

To learn more about how PCI Plus eliminates time-consuming compliance paperwork and costly fees for qualifying merchants, while offering them up to $100,000 in reimbursement costs per MID in the event of a data breach, call **855.613.7085**.



NorthAmerican® BANCARD

PCI Plus

NAB PCI PLUS

PCI DSS COMPLIANT