



Merchant Trust Initiative

Frequently Asked Questions



Frequently Asked Questions

Why is Ezidebit automatically enrolling me into this program?

We are taking a stand against hackers by increasing awareness on cybersecurity and data protection. As a part of this, we need to make sure our merchants are PCI DSS compliant - even if it is not top of mind for you. Our goal is to increase the level of cybersecurity awareness and bring data protection to the front of your mind. As you have a direct agreement with Ezidebit, we have an obligation to ensure you are compliant.

Why is Ezidebit taking a stance on cybersecurity?

Small businesses are the target for over half of all cyberattacks. These attacks are primarily carried out by large-scale criminal organisations based overseas using large workforces and automated tools. The goal of these criminal organisations is to make money by 1) Stealing client information (including credit cards) and selling it, 2) Extorting a ransom from the business to unlock encrypted data, and 3) Stealing funds from accounts. We want to do everything we can to educate and protect you and your business.

What is PCI DSS Compliance?

The Payment Card Industry Data Security Standard (PCI DSS) was created to ensure there is a consistent set of standards for the processing, handling and storing of sensitive credit card information. At Ezidebit, we ensure our payment methods are secure and our processing, storage and transmission of payment data are Level 1 PCI DSS compliant, the highest PCI DSS standard possible.

Which businesses are required to be compliant?

Every business that handles cards, from major enterprises to the smallest businesses, regardless of their size or transaction volume, must ensure they are compliant with the requirements in the PCI DSS. Not doing so may result in suspension from processing cards from certain providers. By staying compliant with PCI DSS requirements, you can be confident that you are doing the right thing by your customers.

How do I know if I'm already PCI DSS compliant?

If you complete a yearly assessment of your PCI DSS status, which is completed using a Self-Assessment Questionnaire (SAQ) accurately, and your assessment shows you have no outstanding actions, then you are PCI-DSS compliant. If you have a portal or e-commerce website, this will include providing evidence of quarterly vulnerability scans from an PCI-SSC approved scanning vendor.

I thought by being with Ezidebit, I was already PCI DSS compliant?

Ezidebit is Level 1 PCI DSS compliant business. However there is a point prior to any of this data being entered into our systems that merchants have an obligation to protect card information. This is part of the reason we are launching the Merchant Trust Initiative - to educate and increase knowledge around these obligations to ensure better cybersecurity and data protection practices.

What are the penalties for PCI DSS non-compliance?

Fines for PCI DSS non-compliance can range from \$5,000 to \$100,000 per month per violation.

How long do I have to become compliant?

You will have 12 months to complete your certification using the TrustKeeper product.

Can I opt out of the initiative?

It is mandatory for all merchants who accept credit cards to be compliant with the PCI Data Security Standard, and this applies regardless of size or how they accept payments. This is not just limited to completing a Self-Assessment Questionnaire (SAQ), but requires a number of steps and regular scans to ensure obligations are met. This is where the Merchant Trust Initiative helps you simplify the steps within the process.

The benefits of the program include giving you access to a number of time-saving tools, resources and proactive monitoring software that aim to support you and give you access to experts along the way.

If you have already met your PCI DSS compliance obligations and choose to opt out of the initiative, go to ezidebit.com/mti-optout and complete the form by 14 December 2018. The form will outline your obligations as a customer of Ezidebit, so please ensure you understand and meet all these requirements prior to opting out.

Does this program guarantee that there will be no chargebacks on my business?

Chargebacks occur for a number of reasons, including the acceptance of stolen cards and failure to deliver goods and services. This program is independent to anything related to chargebacks and as such, does not mean there will be a guarantee of this. The Merchant Trust Initiative relates to educating and improving knowledge around cybersecurity and data protection.

Can you give me more details about the cyber insurance?

More information about the discount offer for cyber liability insurance will be available once the program launches in December.

Where can I get more information about the card scheme rules around PCI DSS compliance?

Each of the card schemes have rules that apply to different members of the supply chain within the payment card industry. The following list from each of the card scheme members outlines their specific rules.




- [Visa](#)
- [MasterCard](#)
- [American Express](#)
- [Discover Financial Services](#)
- [JCB International](#)



Australia

-  www.ezidebit.com.au
-  1300 763 256
-  support@ezidebit.com.au

New Zealand

-  www.ezidebit.co.nz
-  0800 478 483
-  support@ezidebit.co.nz