

Our approach to PCI DSS

A guide for DNA Payments merchants .
Effective 1 September 2026

What's changing from 1 September 2026

Three changes make PCI DSS simpler for most DNA Payments merchants.

01

No SAQ on DNA P2PE devices

If you take payments on a DNA Payments P2PE (point-to-point encrypted) device, you are considered compliant without completing a Self-Assessment Questionnaire (SAQ) unless your volume is in Level 2 [next slide]. Our encryption protects your customers' card data.

02

Security Metrics no longer used

We no longer use Security Metrics to help with SAQ paperwork. Our Onboarding and Account Management teams will tell you which documents, if any, you need to complete. You can terminate any arrangement you have with Security Metrics directly once your contract has ended with them

03

No more PCI charge

DNA Payments no longer charges a PCI fee or a non-compliance fee. New merchants won't pay one, and existing fees are removed at your next price review.

IN SHORT Most small and medium-sized businesses now have nothing to submit and nothing to pay.

Which PCI level are you?

Your level depends on how many card transactions you take each year on each merchant ID (MID). We use the four levels set by the PCI Security Standards Council.

Level	Annual transactions per MID	What you need to provide
Level 1	Over 6 million	Full annual PCI assessment or audit, Attestation of Compliance, and quarterly ASV scans
Level 2	1 million to 6 million	In store: annual SAQ P2PE. Online: annual SAQ A. Plus quarterly ASV scans and additional validation
Level 3	20,000 to 1 million online	Annual SAQ A and quarterly ASV scans
Level 4	Under 20,000 online, or up to 1 million in total	Nothing – no SAQ requested

Most SME merchants are Level 4. If that's you, there is nothing to submit. ASV scans are quarterly vulnerability scans by an Approved Scanning Vendor.

Are you compliant?

✓ Compliant

- Level 1 to 3: all your documents have been received and are up to date – we will direct what we require
- Level 4: no documents are needed, so you are compliant

✗ Non-compliant

- Level 1 to 3: you have not sent your documents, or they are out of date – we will be chasing you
- Keep your SAQ and scans current to stay compliant

How you take online payments matters

The way your website or app connects to DNA Payments can change which SAQ you need. We'll explain this during onboarding and integration.

USING PAY BY LINK?

Pay by Link uses a hosted DNA Payments page, so it does not count as ecommerce for PCI purposes.

Your questions: fees and Security Metrics

Q I currently pay a PCI fee. Will it stop?

New merchants are not charged a PCI fee.

If you already pay one, it continues until your next scheduled price review, when it will be adjusted.

Q I'm enrolled with Security Metrics. What happens now?

It's your choice. If you still want their support, you can work with Security Metrics directly and pay for their service.

Q My partner or software provider charges me a PCI fee. Is that right?

DNA Payments does not charge a PCI fee, but partners may charge for services they provide – for example, helping you complete your SAQ as part of their integration.

A partner should not charge you a non-compliance fee where DNA Payments considers you compliant or does not require an SAQ.

Your questions: SAQs and changes to your level

Q Can DNA Payments fill in my SAQ for me?

No. You must complete your SAQ yourself, as the answers must reflect how your business handles card data.

We can provide advice but we cannot complete for you.

Q What happens if my PCI level changes?

Our Account Management team reviews levels every quarter and will tell you if what we need from you has changed.

Q What happens when I join DNA Payments?

Your DNA Payments contact will explain your PCI requirements. If you need an SAQ, you'll share it with us during onboarding.

Q Who do I ask if I'm not sure?

Contact your Account Manager or the DNA Payments team who onboarded you.

Taking card details over the phone (MOTO)

Mail order and telephone order (MOTO) payments are the highest-risk transactions we process. That's why we have a separate MOTO Policy.

01

Higher risk of fraud

MOTO payments skip the usual checks – Chip and PIN in store and 3D Secure online – so you have little defence if a customer raises a chargeback.

02

Card data at risk

You key the card number, security code and expiry date into a terminal yourself, so these details can be misused if they are recorded anywhere.

GOLDEN RULE: NEVER RECORD CARD DETAILS

- ✗ Don't write card details down
- ✗ Don't type them into a computer, spreadsheet or email
- ✗ Don't photograph a card or store card details in any form

Your PCI checklist

If you...	What to do
Use DNA P2PE devices and are Level 4	Nothing to submit – you are compliant
Take more than 20,000 online transactions a year	Complete an annual SAQ A and quarterly ASV scans
Take over 1 million transactions a year	Check the Level 1 or 2 requirements and keep your documents up to date
Take payments by phone or mail (MOTO)	Follow the MOTO Policy – never record card details
Currently pay a PCI fee to DNA Payments	No action – it is adjusted at your next price review
Need help with an SAQ	Contact your Account Manager for high level guidance or visit the PCI Website

Questions? Contact your DNA Payments Account Manager.