



MERCHANT GUIDE

Protecting your online payments from BIN bashing

How card-testing attacks work, the warning signs to watch for, and what to do if your checkout is targeted.



24/7 SUPPORT

0800 729 627

If an attack may be happening, call Paymark straight away.
Don't refund or reverse unexpected transactions until you've spoken with us.

01 | UNDERSTANDING THE THREAT

What is BIN bashing?

BIN bashing is a form of ecommerce fraud where criminals use automated attempts to test combinations of card details through online payment environments.

A BIN (Bank Identification Number) is the first 6 to 8 digits of a card number, and it identifies the bank that issued the card. Criminals start with a known BIN and use software to guess the remaining digits, the expiry date and the security code. They then push those guesses through an online checkout to find out which numbers work.

01**Pick a BIN**

Criminal starts from a known card issuer number range.

02**Generate details**

Software creates card number, expiry and CVV combinations.

03**Test at scale**

Bots push rapid attempts through an online checkout.

04**Exploit**

Approved card details are used for fraud or sold on.

02 | TAKING ACTION

What you can do

ATTACK HAPPENING NOW?

Call Paymark 24/7 support on **0800 729 627**. Don't refund or reverse any unexpected transactions until you've spoken with us.

To reduce the risk and cost of an attack, do these four things: check your fraud protections, add protections to your website, watch for warning signs, and act quickly if something doesn't look right.

1 Check your fraud protections

- **Check that 3-D Secure (3DS) is turned on for your account.** Paymark sets up 3DS when your account is created, and you can't change it in the Portal. Most Paymark ecommerce merchants have 3DS turned on by default.
- **With 3DS, customers might see an extra verification step when they pay.** If you're not sure whether you have 3DS, contact Paymark support.
- **If your website, platform or checkout changes,** review your settings again.

3DS works alongside other fraud controls, but it doesn't stop automated payment attempts against your checkout. To slow those attempts down, add protections to your website.

2 Add protections to your website

Paymark's fraud controls are one layer of protection. Your website and checkout are another important line of defence. Where possible, stopping automated attempts before they reach the payment platform can help reduce the impact of an attack. Depending on your setup, ask your web developer or platform provider about:

- CAPTCHA or bot protection, particularly after repeated failed attempts
- Rate limiting on payment and checkout submissions
- A web application firewall (WAF) or equivalent website security controls
- Controls around repeated attempts from the same IP address or device
- Requiring customers to sign in or using additional verification where appropriate
- Monitoring and alerting for sudden spikes or unusual website and checkout activity
- Keeping plugins and integrations up to date

3 Watch for warning signs

One sign on its own doesn't necessarily mean you're experiencing an attack. Look for unusual patterns or combinations of activity, and contact Paymark if you're unsure.

Warning sign	What it can look like
Spike in declined transactions	Far more declines than usual in a short period
Many low-value attempts	Repeated small or zero-value payments you don't recognise
Sudden increase in transaction activity	A large number of payment attempts within a short period
Repeated order/reference numbers	Multiple payment attempts against the same order or reference, which may indicate repeated checkout submissions
Repeat IP address or device	Many attempts from one source, or a handful of sources
Repeated card ranges	Multiple attempts using cards from the same or similar number range. Your visibility of this may depend on your setup.
Activity at unusual times	Bursts of attempts overnight or outside your normal trading pattern
Repeated transaction amounts	Many attempts for the same or similar amount, potentially across different orders

4 Act quickly if something doesn't look right

- Call Paymark 24/7 support straight away on 0800 729 627, or email support@paymark.co.nz.
- Don't refund or reverse unexpected transactions until you have spoken with us.

- **Ask your web developer or platform provider to tighten bot protection.** Consider CAPTCHA, rate limiting or other controls to slow automated attempts reaching your checkout.
- **Work with Paymark to block cards, card ranges or countries associated with the attack** where appropriate.
- **Keep a note of what you saw and when**, including transaction or order references, times, amounts, IP addresses and screenshots.

03 | THE IMPACT

Why does it matter?

An attack can create a large number of payment attempts in a short time. That can affect your business in four ways:

Costs

Transaction or processing fees on attempted payments, and chargebacks if stolen card details are used successfully.

Disruption

Time spent investigating, reconciling and cleaning up unusual activity, and a possible slowdown of your checkout.

Customer impact

Genuine customers may see declines or delays, which can affect trust in your online store.

Wider impact

Card details confirmed through your checkout can go on to be used against cardholders elsewhere.

04 | OUR SUPPORT

What support is available from Paymark?

Controls available to you

Control	Available today?	Recommendation
Velocity / fraud-management rules	YES	RECOMMENDED
3DS (3-D Secure)	YES	RECOMMENDED
Optional advanced fraud service (Forter)	YES	OPTIONAL

How we monitor and alert

Paymark monitors transaction activity for patterns that can indicate unusual or potentially fraudulent activity and may take steps to help reduce the impact where suspicious activity is identified.

Fees and costs

BIN bashing can generate a high volume of failed transaction attempts, which may result in unexpected transaction fees. If we confirm that fees came from a BIN bashing attack, we review them case by case. We take into account the circumstances and the steps taken to address the attack. Report unusual activity straight away, and keep a record of what you saw.

How the layers work together

3DS (3-D Secure)	Applied based on risk, so customers only see an extra step where risk requires it. Lower fraud exposure and liability shift where applicable, with minimal impact on conversion.
Velocity / fraud-management rules	Real-time limits on amounts, attempts and spend over time, card and country blocking, and refund controls. Immediate protection against card testing and rapid-fire fraud.
Forter (optional partner service)	Behavioural analytics and real-time risk scoring using device, identity and transaction signals. Suits high-volume, cross-border and repeat-purchase merchants. Fees are agreed directly with Forter.

You can use one or all of these layers, depending on your risk profile, transaction volumes and growth stage.

During and after an attack

What we do during an attack

A specialist support team will look into what's happening. They check transaction activity, the card ranges being used and when it started. If it's serious, they bring in our ecommerce technical team.

Click has built-in fraud controls. During an attack we can work with you to set or tighten:

- **Transaction limits.** Minimum and maximum amounts for each transaction.
- **Account limits.** Caps on the total value or number of transactions over a set period.
- **Card limits.** Caps on how many successful or unsuccessful attempts one card can make, and how much it can spend, within a set time.
- **Card blocking.** Block a specific card, the card used in a transaction, or cards issued in a particular country.

We'll keep you updated while we investigate and tell you what we found. If you have an account manager, we'll keep them in the loop too.

After an attack

Once the activity has stopped, we'll share what we found. That covers when it happened, how many transactions were involved and which card ranges were targeted. We'll also recommend changes to your setup to reduce the risk of it happening again. These could include permanent limits, card or country blocking, 3DS if you don't already use it, or Forter for advanced fraud screening.

Forter is a separate partner service with its own fees, agreed directly between you and Forter.

05 | GET HELP

Who to contact

If you think your online store is experiencing BIN bashing, contact our 24/7 Support team straight away. If the activity is still happening, call us so we can start investigating straight away. You don't need to be sure it's fraud.

PHONE · 24/7

0800 729 627

Best option if an attack is in progress

EMAIL

support@paymark.co.nz

For follow-ups and non-urgent queries

When you get in touch, have ready:

- Your merchant ID
- Example order or transaction numbers
- The approximate time the activity started
- Any relevant screenshots, IP addresses or amounts

Moving Payments Forward. Together.