

What to do right now

Think your business is experiencing a BIN-bashing attack? Work through these steps and tick them off as you go.

01 Spot the signs

WATCH FOR

- A sudden spike in transaction attempts
- A high number of declined transactions
- Many small or identical amounts

ALSO LOOK FOR

- Many different cards in a short time
- Repeated attempts from one IP address or device
- Activity outside normal trading hours

02 Act now

- ☐ **Contact the Paymark team.** The sooner we know, the sooner we can help.
0800 729 627 · support@paymark.co.nz
- ☐ **Tighten your velocity rules.** Lower the limit on unsuccessful attempts and the number of transactions allowed in a set time.
- ☐ **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.
- ☐ **Check 3DS authentication is switched on** for your online payments.
- ☐ **Work with Paymark to block cards, card ranges or countries associated with the attack** where appropriate, including countries you don't sell to.
- ☐ **Don't refund or reverse unexpected transactions** until you've spoken with Paymark.
- ☐ **Record what you've seen.** Note times, transaction references, amounts, IP addresses and screenshots.

03 Follow up

- ☐ **Keep monitoring your transactions** after the activity stops, in case it returns.
- ☐ **Review your fraud settings with us** and check they suit your business, including whether advanced fraud detection would help.
- ☐ **Review your website and checkout protections** with your web developer or platform provider.

WE'RE HERE TO HELP

If something doesn't look right, contact Paymark on **0800 729 627** or **support@paymark.co.nz**.