E-commerce fraud defence: A quick guide for merchants

ecommpay

E-commerce has revolutionised how we transact, but alongside the benefits of digital payments come significant risks. In 2024 alone, payment fraud losses in the UK reached £1.17 billion.

Every fraudulent transaction costs merchants far more than the lost revenue, impacting profitability, reputation, and payment processing capabilities. This guide outlines the 9 most critical fraud threats facing businesses today and provides proven strategies to stop them.

1

Identity theft

The problem

Fraudsters steal consumer data through phishing or hacking to impersonate legitimate customers. Using stolen names, emails, and payment details, they make unauthorised purchases that leave merchants liable.

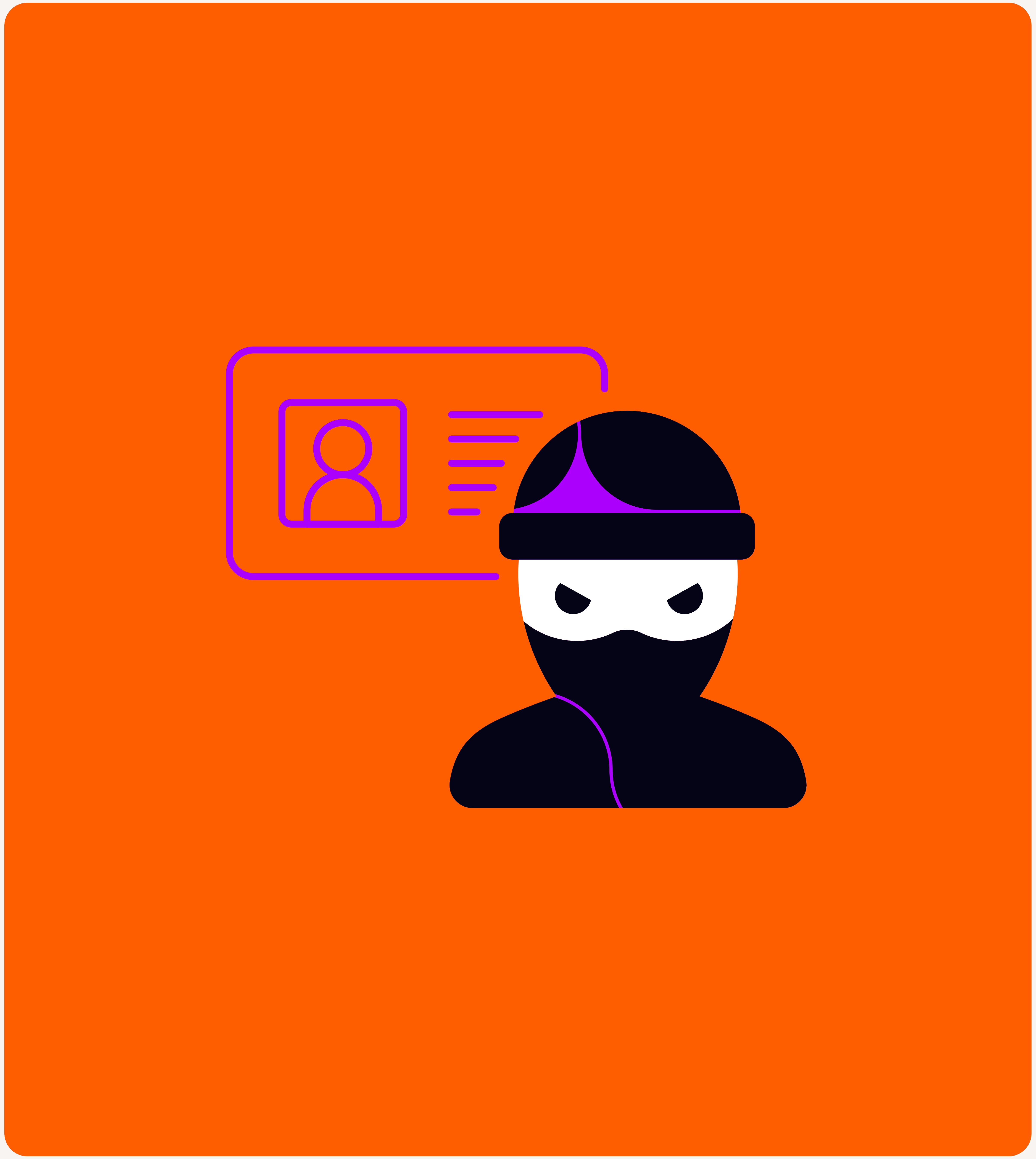
How to avoid it

Verify identities
Use 3D Secure 2 (3DS2) to authenticate cardholders in real-time.

Educate customers
Remind users to check for trust signals and avoid sharing sensitive data via email or social media.

Monitor velocity
Flag multiple orders placed rapidly from the same IP address or device.

Add enhanced checks for high-value purchases
Consider AI fraud detection tools or video verification for higher-risk / high-value transactions.



2

Friendly fraud

The problem

A customer makes a purchase but later disputes the charge, claiming it was unauthorised or never received. This is often done to keep the item for free or because they simply forgot about the transaction. It accounts for 45% of all chargebacks.

How to avoid it

Use clear billing descriptors

Ensure your business name appears clearly on bank statements to prevent confusion.

Communicate proactively

Send immediate order confirmations, tracking numbers, and delivery updates.

Keep robust records

Maintain logs of IP addresses, delivery confirmation, and communications to dispute invalid claims.

Use real-time delivery tracking

Keep live delivery status records to support evidence in chargeback disputes.

3

Refund fraud

The problem

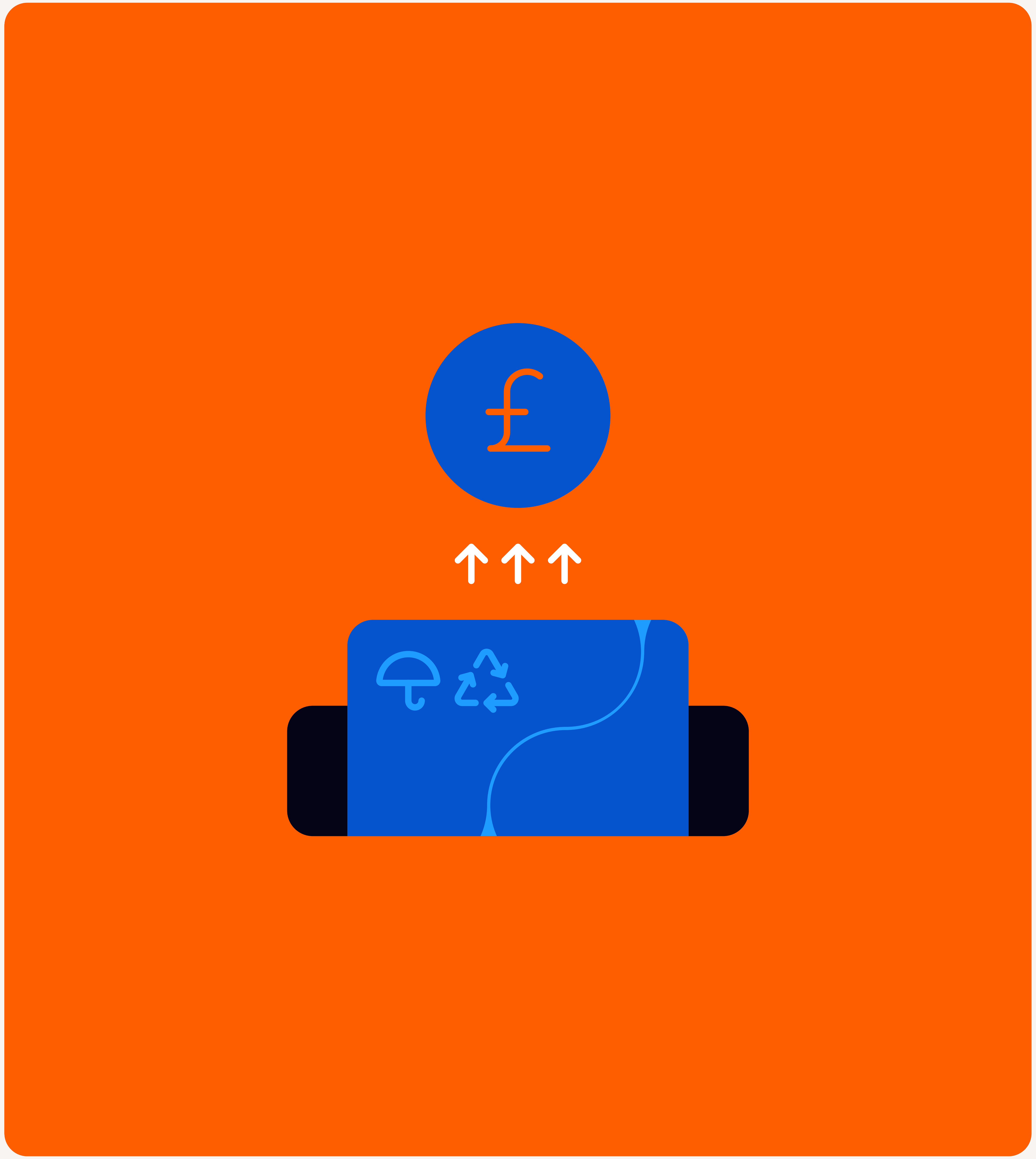
Criminals exploit return policies to secure refunds for stolen goods, return empty boxes, or use "decoy" returns (returning counterfeit items). In 2024, fraudulent returns accounted for an estimated £103 billion globally.

How to avoid it

Enforce a strict policy
Publish a clear returns policy that demands receipts and proof of purchase.

Inspect before refunding
Verify the condition of returned items before releasing funds.

Track serial returners
Use fraud detection tools to identify customers with suspicious return histories.



4

Business email compromise (BEC)

The problem

Fraudsters compromise legitimate business email accounts or impersonate senior executives to trick employees into authorising fraudulent payments or changing supplier bank details.

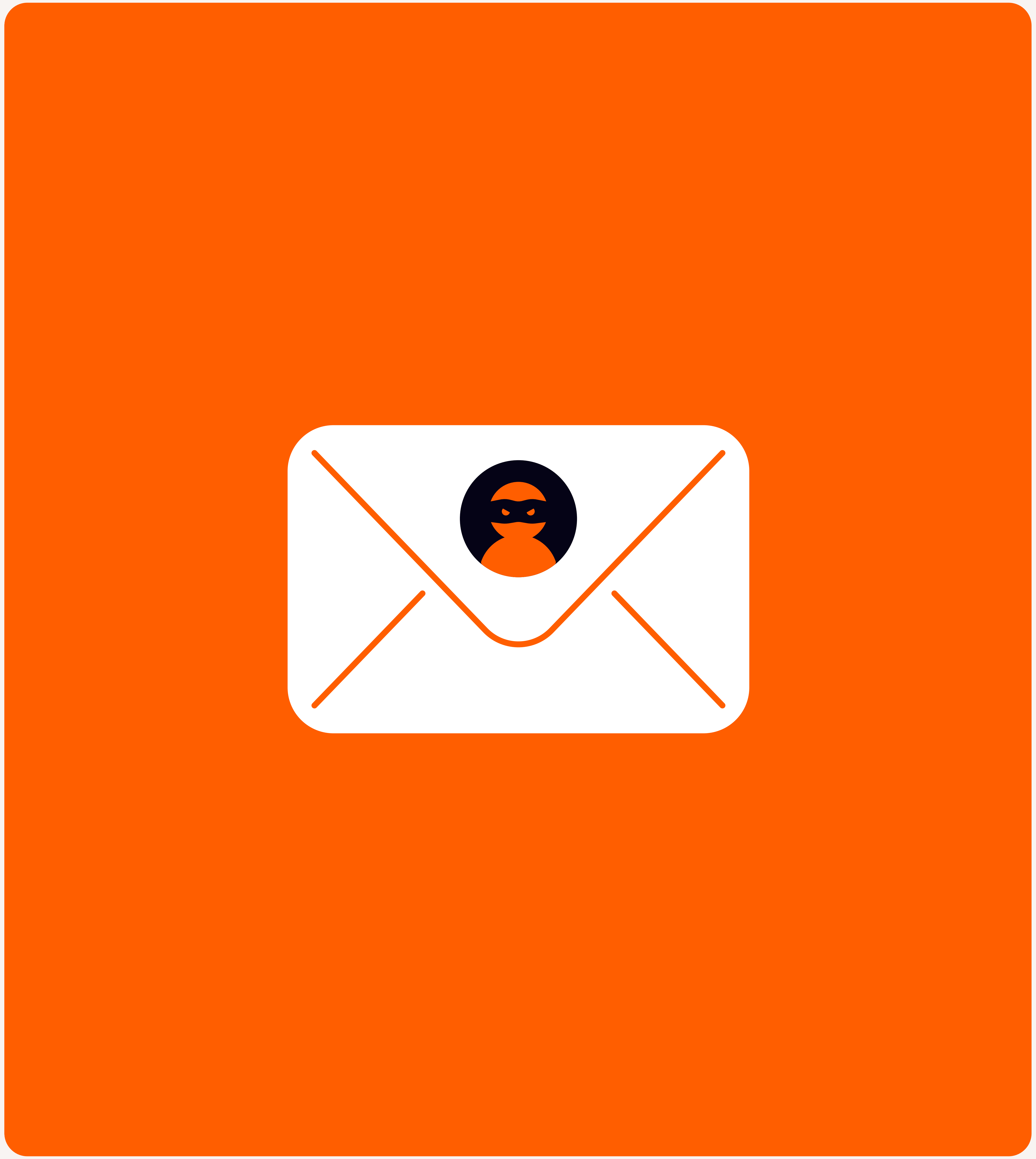
How to avoid it

Train your staff
Educate employees to spot phishing attempts and inconsistent email addresses.

Verify requests
Mandate phone verification for any request to change payment details or transfer funds.

Use dual authorisation
Require approval from two people for high-value transactions.

Strengthen technical controls
Use strong data security, multi-factor authentication (MFA), and appropriate technical safeguards to protect business email accounts.



5

Payment interception

The problem

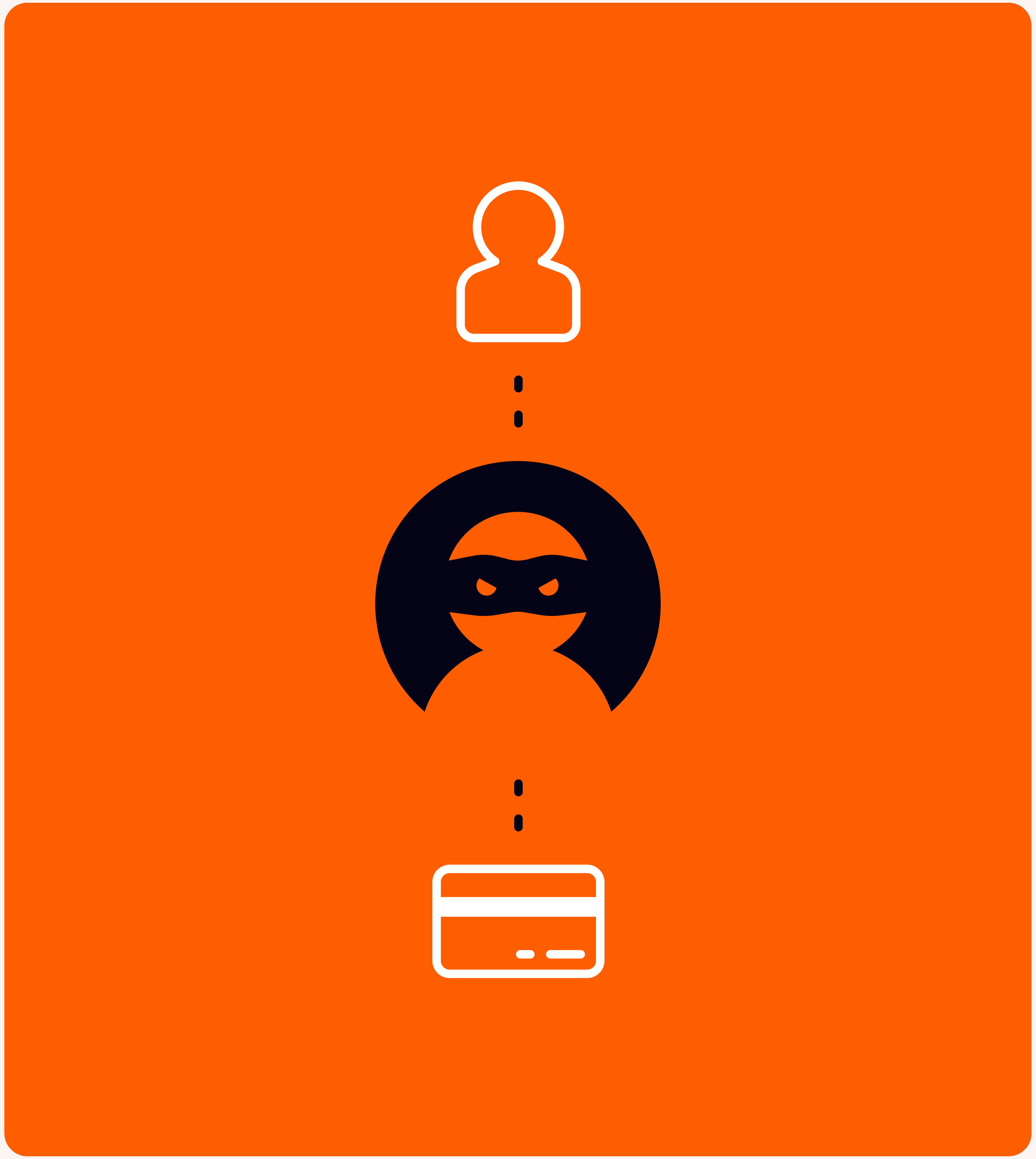
Also known as "man-in-the-middle" attacks, hackers hijack the payment process or redirect customers to fake payment pages to steal data. This is increasingly common with real-time payments.

How to avoid it

Secure your gateway
Only use trusted payment partners with strong security controls, fraud monitoring, and secure payment page protections.

Educate users
Warn customers that you will never ask for payments via unsolicited links or social media.

Set velocity limits
Restrict the number of transactions allowed in a short period to block automated attacks.



6

Password or code hacking

The problem

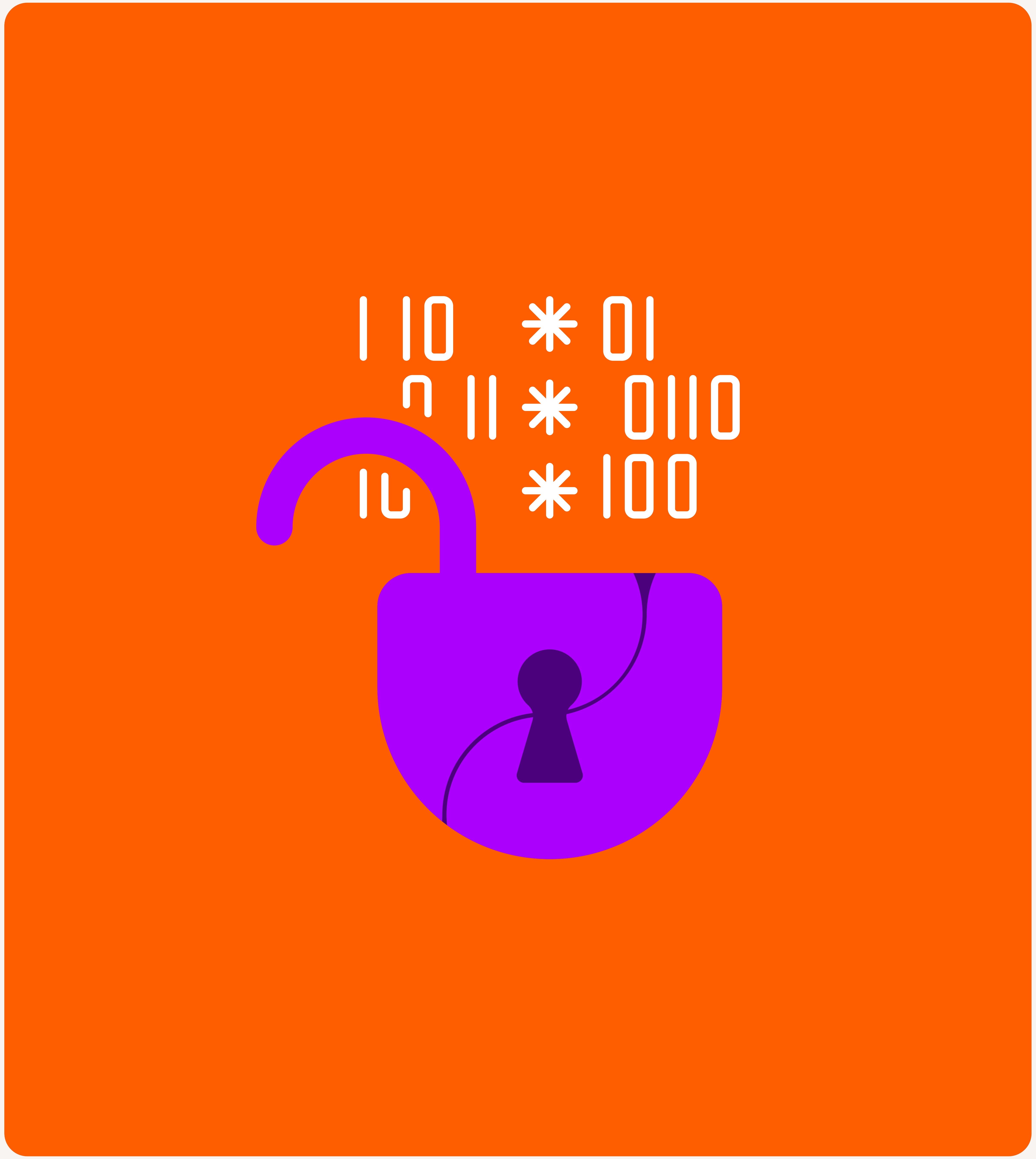
Scammers use sophisticated tools to capture login credentials, often exploiting weak passwords or reused credentials from other data breaches. 52% of login attempts now involve previously leaked credentials.

How to avoid it

Enforce strong passwords
Require complex passwords and encourage the use of password managers.

Enable multi-factor authentication (MFA)
Use MFA for logins and sensitive account changes.

Secure infrastructure
Partner with PCI DSS Level 1 certified providers to ensure data safety.



7

Website takeovers

The problem

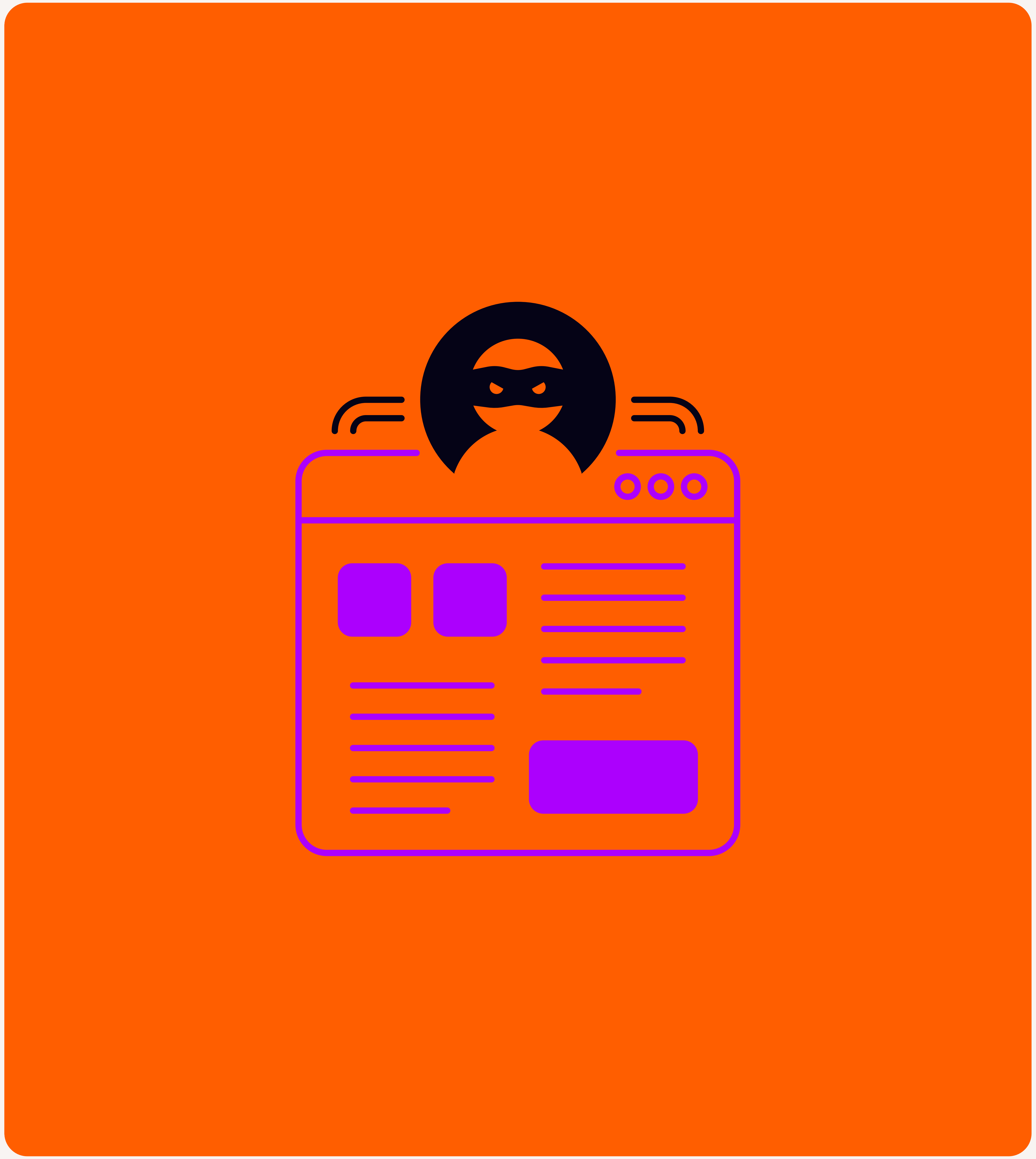
Hackers gain administrative access to an e-commerce store, often through outdated plugins or weak passwords. They then redirect payments to their own accounts or steal customer data directly from the source.

How to avoid it

Audit plugins regularly
Remove unused apps and keep all software patched and up to date.

Use a web application firewall (WAF)
Block malicious traffic before it reaches your store.

Isolate payments
Use hosted payment pages to separate processing from your main website infrastructure.



8

Account takeover (ATO)

The problem

Fraudsters gain access to a legitimate customer's account to make purchases, drain loyalty points, or lock out the real owner. ATO attacks increased by 76% in 2024.

How to avoid it

Deploy behavioural analytics
Flag logins from new devices, locations, or unusual times.

Stop credential stuffing
Use CAPTCHA and rate limiting to prevent automated login attempts.

Monitor anomalies
Watch for sudden changes to contact information followed immediately by high-value orders.

Use identity verification tools
Apply step-up identity checks for suspicious logins, account recovery, or high-risk account changes.

9

AI-powered fraud and deepfakes

The problem

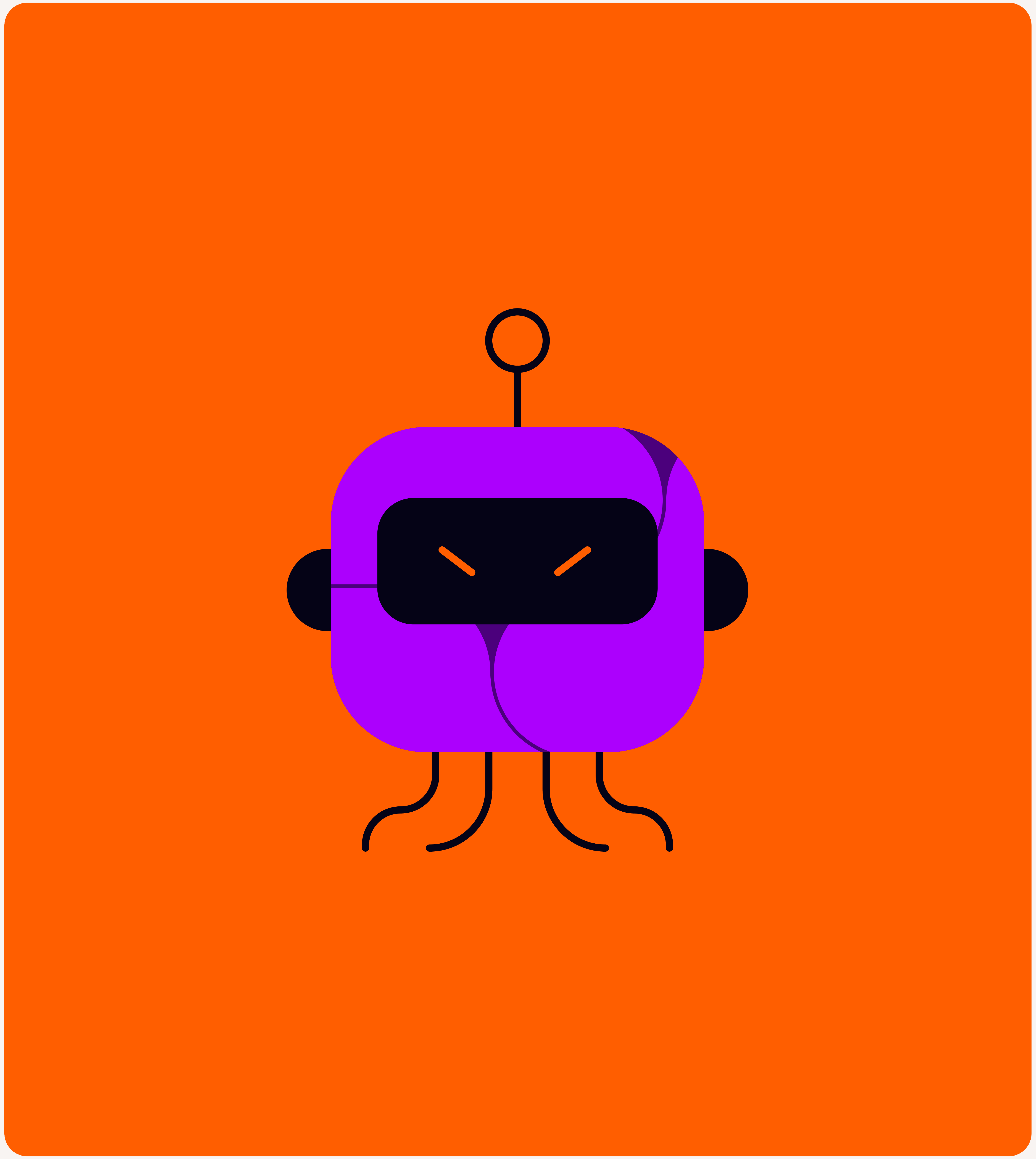
Criminals use generative AI to create convincing phishing emails, forged documents, and deepfake videos to bypass verification checks. Over 50% of fraud now involves AI tools.

How to avoid it

Fight AI with AI
Use specific detection tools that spot subtle anomalies and non-human patterns in real-time.

Use liveness detection
Require real-time interaction for identity verification rather than static images.

Verify "out-of-band"
Confirm urgent video or voice requests via a separate, trusted communication channel.



Protecting your business

The most effective defence is a multi-layered approach. Partner with a payment provider that prioritises security through:

- AI-powered fraud detection to spot suspicious patterns.
- Tokenization to protect customer data.
- 3D Secure 2.0 for robust authentication.
- Real-time monitoring to block threats instantly.

Take the next step

Ecommpay's award-winning risk management platform combines advanced technology with expert human oversight to deliver a 97%+ fraud prevention rate. Speak to our experts today to secure your revenue.

Let's chat! →