Payment Fraud Prevention Checklist – helping your business stay secure

Focussed on payments, this quick checklist helps small businesses stay one step ahead with smart, scalable fraud protection tactics. Use it to train your team, tighten your processes, and help protect your profits.

At checkout: Secure the transaction

- **Use Chip & Pin or contactless to reduce chargeback risk**

  These methods are more secure and help prove customer presence, making it harder for fraudsters to dispute transactions. Be particularly mindful of customers wanting to pay remotely and collect in person.

- **Consider using Pay-by-Link so that payments are taken securely**

  Pay-by-Link helps businesses avoid card-not-present fraud, such as stolen card use, social engineering, and mis-keyed card details during phone payments.

- **Check your ecommerce software is fit for purpose**

  Make sure you're using the right level of software if you're taking online payments. Speak to your payment services provider to make sure you have a secure payment gateway and the fraud prevention tools you need.

- **Make sure you're compliant with industry standards**

  Check your PCI DSS compliance is up to date and keep on top of software updates as this can help minimise risk.

- **Train colleagues to spot unusual transactions and scams**

  Help employees recognise red flags like mismatched cardholder details, rushed purchases, or unusually large orders, to prevent fraud before it happens.

- **Secure supervisor cards and terminal access codes**

  Keep high-level access credentials locked away and limit who can use them to avoid unauthorised overrides or refunds.

- **Watch for distraction techniques at the point of sale**

  Be alert to tactics like rushed conversations or multiple people engaging staff, which can be used to divert attention during a scam.

- **Keep devices updated and plugins current**

  Regular updates patch security vulnerabilities and help keep your systems protected against the latest threats.

LLOYDS

Post-checkout: Protect against follow-up fraud

- **Stay alert with new accounts**
  Keep an eye on new accounts that are set up, to spot any unusual behaviour before it has chance to escalate.
- **Don't dispatch goods until identity and address are verified**
  Confirm customer details – especially for high-value orders – to avoid sending products to fraudulent or unverifiable addresses.
- **Run quick sessions on handling declined payments and refunds**
  Equip staff with clear steps to follow when payments fail or customers request refunds, reducing confusion and potential manipulation.
- **Review fraud trends and update safeguards accordingly**
  Stay informed about emerging scams and adjust your processes to stay one step ahead of fraudsters.

Keep fraud at bay – all year long

Stay alert, and regularly review your payment fraud safeguards throughout the year. Keep this checklist handy, share it with your team, and revisit it often to help stay secure.

Want more of a deep dive?

Take a look at our **PSI DSS compliance** page to find out more about how this safeguards your customers and your business.

Business help and support

We aim to provide you with a high level of service. If you have a query our Help & Support pages can help: **lloydsbank.com/business/help**

Please contact us if you would like this information in an alternative format such as braille, large print or audio.

61729 (10/25)