Credicorp
Suite 53C Unimix House
Abbey Road
London NW10 7TR
www.credicorp.co.uk
support@credicorp.co.uk

30 May 2026

Payment security

Payment Security (PCI-DSS) Statement

Reference: PCI-DSS

Version 1.0 - last revised 25 May 2026

Keeping your company's payment details safe is a basic responsibility. This statement explains how we handle that data and the standards we hold ourselves and our providers to.

How repayments are taken

Repayments are collected by Direct Debit from the company's nominated UK business bank account, under the BACS Direct Debit Guarantee. We hold the sort code and account number needed to set up the mandate; we do not need or store full payment-card numbers to run a Direct Debit.

If a card payment is offered

Where a card payment is offered, it is processed by a PCI-DSS compliant payment provider. Card details are entered directly with that provider; full card numbers are not stored on our systems. This keeps our card-data environment to the smallest possible scope.
Our card payment provider is Stripe. For how we follow Stripe's Restricted-Businesses and acceptable-use rules, and how your right to dispute a card charge with your bank works alongside our own complaints process, see our Stripe Acceptable-Use Adherence Statement.

How we protect data

- Data is encrypted in transit (HTTPS/TLS) across the site, the customer portal and the staff workspace.
- Access to customer financial data is limited to staff who need it for their role, and important actions are recorded in an audit log.
- Bank-statement data shared for affordability is used only for that assessment and retained under the retention rules in our Privacy Notice.
- We do not sell payment or personal data.

Reporting a security concern

If you believe any payment or account data has been exposed, contact us immediately at security@credicorp.co.uk so we can investigate. You can also raise a concern through our Complaints Procedure.
ICO Registration No. ZC157682