shieldpay

Trust & Security Guide

Ensuring trust and security for the Payments That Matter™

Version 2, December 2025

CLASSIFICATION: CONFIDENTIAL

Contents

Introduction from our CEO

Sophie Condie
Chief Executive Officer

At Shieldpay, we recognise that trust is the foundation of our relationship with customers, partners, payers and payees. As an FCA-regulated payment institution, we are committed to maintaining the highest standards of security, transparency, and regulatory compliance, to ensure the security of the funds we hold and personal data we process, along with the integrity of our services.

Security and operational resilience are embedded in everything we do, from our robust encryption and access controls to continuous monitoring and threat detection. We follow industry best practices, including compliance with FCA regulations and guidance, data protection legislation, and internationally recognised standards such as ISO 27001, ensuring our services meet the stringent requirements expected of a leading payment services provider.

Compliance is not just a requirement - it is a core principle that drives our business operations. We actively review and update our policies to align with evolving regulatory standards and security threats. Our team undergoes regular training, and we engage external auditors to validate our compliance and security posture.

We believe in transparency and proactive communication. If you have any questions or concerns regarding our security and compliance practices, our dedicated security and compliance teams are here to assist.

By upholding these commitments, we empower our customers with confidence in our services and platform, ensuring safe, reliable, and compliant solutions for their business needs.

Sophie

Business continuity and disaster recovery

We have implemented robust business continuity (**BC**) and disaster recovery (**DR**) processes to ensure that we can prevent, respond to, recover, and learn from, operational disruptions, while maintaining the integrity of essential business services.

Our BC/DR measures are comprehensive and include several key components:

Recovery objectives: We have defined Recovery Time Objective (**RTO**) and Recovery Point Objectives (**RPO**) for our services. For example, the database for our payments platform has an RTO of 30 minutes and an RPO of 1 day, while our API has an RTO of 2 hours.

Cross-regional back-ups: Databases for our treasury, onboarding and [party] services have replicas in different availability zones within the UK and EEA to protect against physical harm.

Automated restore workflows: We have developed workflows for cross-regional database restoration from snapshots, allowing for quick recovery. The database for our payments platform can be restored in 15 minutes.

Game day scenarios: Regular testing through ‘gameday’ scenarios ensures readiness for disaster recovery. These scenarios simulate incidents to test the effectiveness of recovery procedures.

Business continuity planning: We maintain a detailed business continuity plan which establishes clear actions across all levels of the business to support the business through advised events.

Our BC/DR plans are subject to periodic review and refresh to ensure they remain current. The review process involves consideration of key inputs such as the outcomes of quarterly gamedays as well as ‘incidents’ raised since the last review, to ensure those plans reflect new and emerging risks that have been identified.

Data protection

Our role

As an FCA-regulated payment institution, we are required to comply with the Payment Services Regulations 2017 and related guidance published by the FCA. We are also a 'relevant body' under the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017, requiring us to implement effective systems and controls to prevent our services from being used for money laundering or terrorist financing purposes.

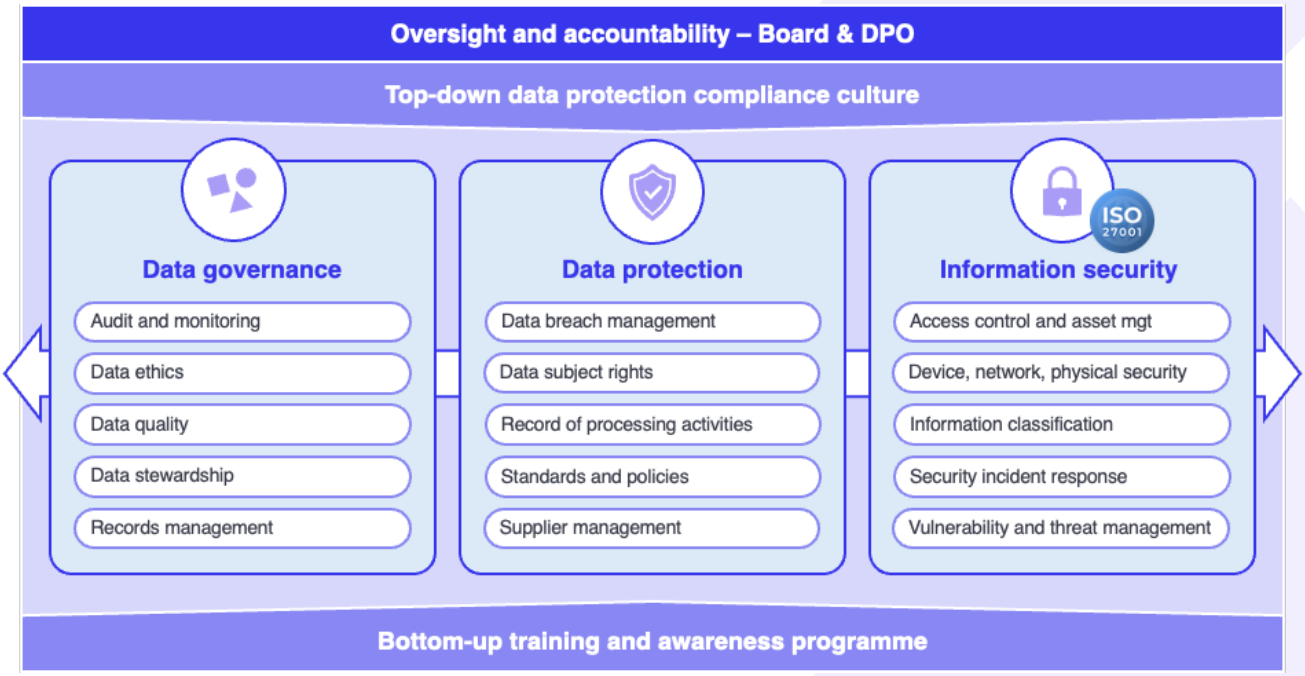
While we may provide payment services on behalf of our customers, we determine the purposes (the 'why') and the means (the 'how') of processing personal data relating to payers and payees, in the context of providing our services.

As a 'controller', we are accountable (in accordance with the principle set out in Article 5(2) UK GDPR) for the lawful processing of, and effective and comprehensive protection of, personal data. This, in turn, affords the greatest degree of protection to payers and payees, ensuring the full effect and benefit of data protection law for them.

Our staff are employed or engaged by Shieldpay Operations Limited, which is a wholly owned subsidiary of the same parent company as Shieldpay Ltd. There is an Intercompany Data Processing Agreement in place between these two companies.

Data protection framework

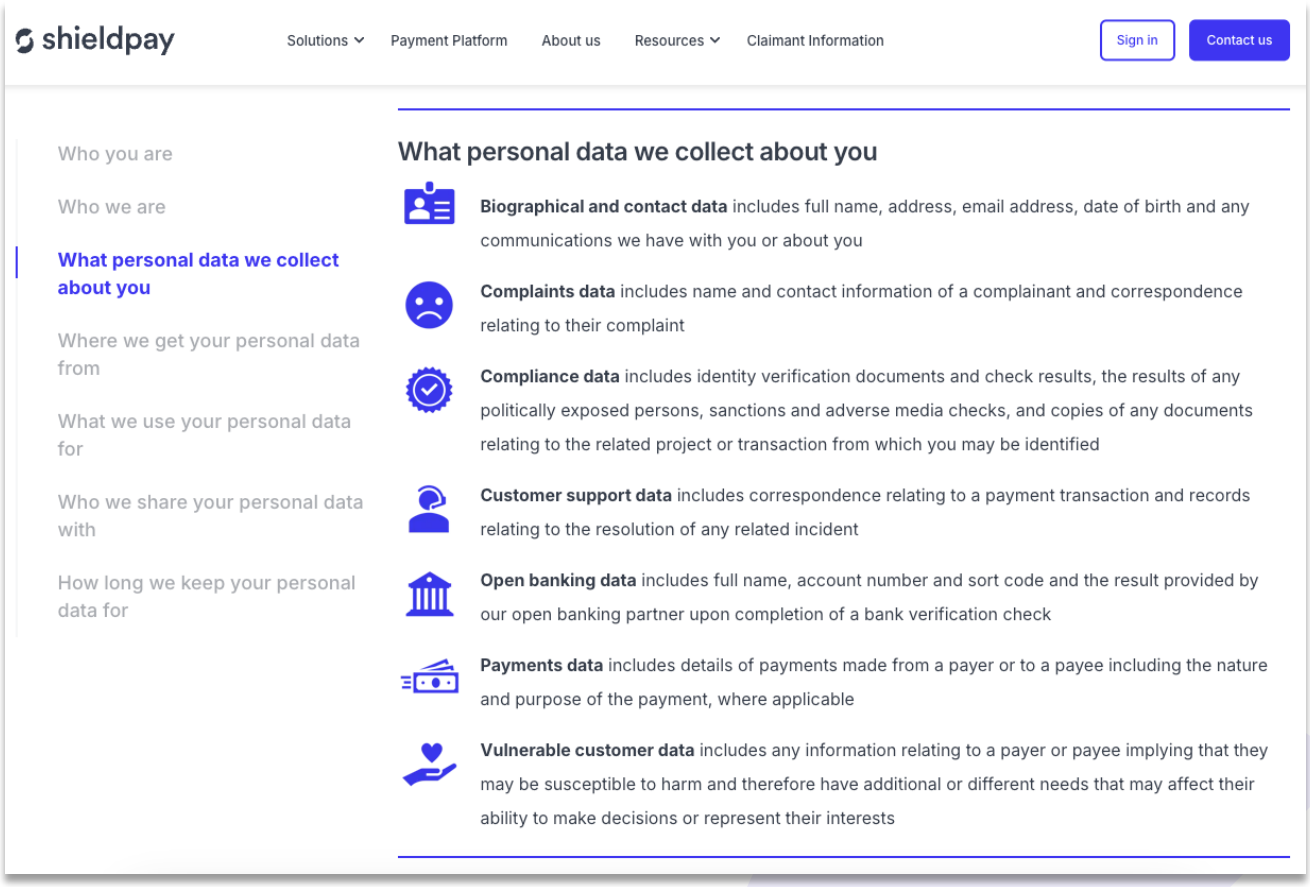
Shieldpay has implemented a robust data protection framework which is owned and overseen by its Data Protection Officer:



Ensuring transparency

Our goal is to ensure that no-one is surprised by what personal data we have collected about them or how we use it. Our Privacy Notice makes it easy for individuals to find out more about how we process their personal data, with the use of icons making it clear which categories of personal data we use for each purpose we use it for.

Our Privacy Notice is reviewed at least annually and is updated when there are any changes to how we collect and process personal data.



Fraud and financial crime prevention

Our approach

The FCA Handbook requires us to take reasonable care to establish and maintain effective systems and controls for compliance with applicable requirements and standards under the regulatory system, and for countering the risk that we might be used to further financial crime.

Our Fraud Policy articulates a zero-tolerance approach to fraud and financial crime, which directs the 'tone from the top'. We are committed to maintaining an active culture of fraud awareness, encouraging personnel and customers to report any suspicious activity to protect against financial loss and the associated disruption and detriment associated with fraudulent activity.

Specific fraud and financial crime risks

Our financial crime framework mitigates a wide variety of financial crime topologies, including the following key risks we face as a payment institution:

Authorised push payment (APP) fraud

APP fraud occurs when a person uses a fraudulent or dishonest act or course of conduct to manipulate, deceive or persuade someone from transferring funds from one UK bank to another, where either the recipient was not the intended payee, or the payment was not for the purpose intended by the payer.

Our solution combines multi-factor authentication, advanced role-based access control, audit trails, Confirmation of Payee (CoP) checks and automated transaction monitoring to significantly reduce the risk of APP fraud taking place.

Cybersecurity breaches

A cybersecurity breach may involve a brute force attack on our platform and systems by a malicious third-party actor, or an email scam directed towards our employees

We have implemented an information security management system which has been certified to the ISO27001 international standard. This system establishes protocols for cloud and network security, threat intelligence, malware prevention and secure software development and testing procedures. We maintain a continual security improvement policy designed to address security issues and vulnerabilities, while preventing (re-)occurrence.

Fraudulent approvals and documents

Users of our platform may attempt to make fraudulent payments if they have the relevant permissions, and parties to transactions may falsify release instructions.

We have implemented robust systems and controls to spot potentially fraudulent transactions on our platform, requiring changes to payment details to be verified by approved individuals. Release Instructions are carefully reviewed to ensure they've been signed by the nominated Authorised Signatories.

Financial crime procedures and audits

We have implemented a robust framework for the prevention of fraud and financial crime which is overseen by our Chief Compliance Officer. Staff receive training on our financial crime procedures when the first join Shieldpay, and at least annually thereafter.

Our AML framework is audited annually by an independent firm of auditors. Our 2024 audit was assessed as 'Green' with an overall score of **99.66%** (2023: 90.48%).

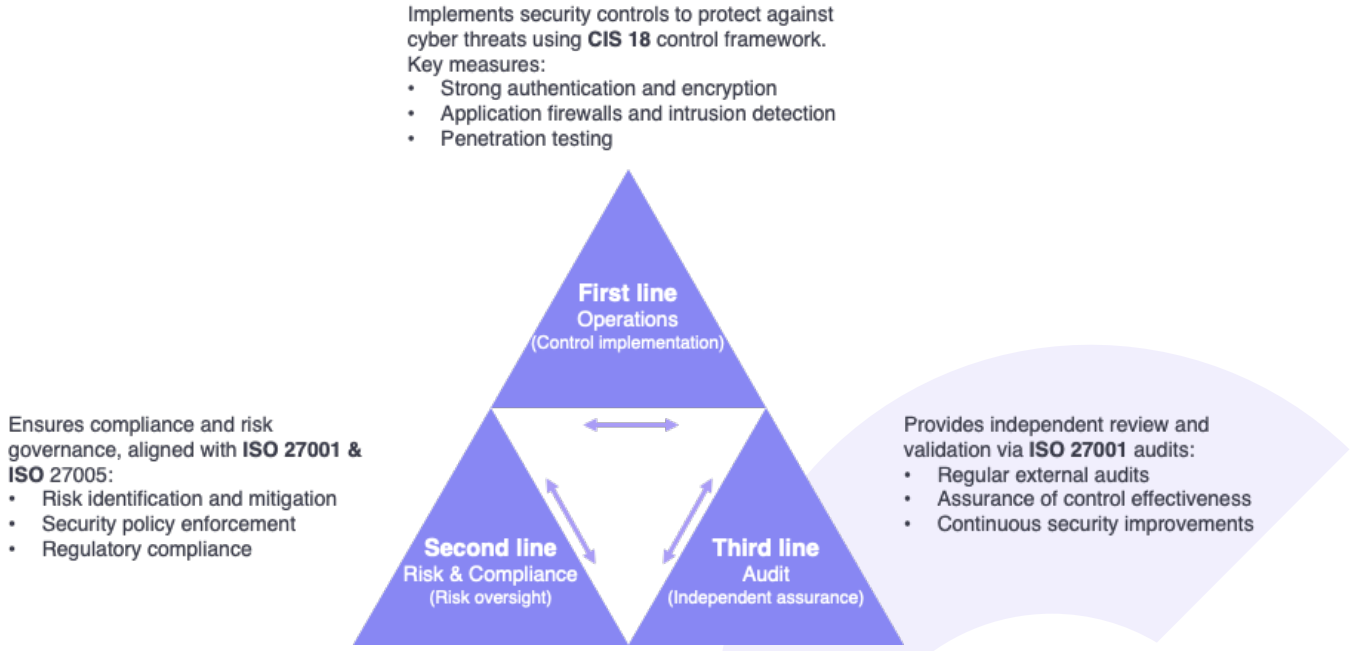
Information and cyber security

Information security framework

Our Information Security framework is built on the 3 lines of defence (3LoD) mode, ensuring accountability and oversight at every level.

Our operational teams form the **first line** by implementing baseline security controls, while our risk and compliance functions serve as the **second line** by monitoring and validating these measures. An independent audit provides the **third line** of assurance, confirming that our systems operate as intended.

This layered approach - supported by comprehensive policies, procedures, governance, and 24/7 security monitoring - ensures data and transactions are protected against evolving threats.



nqa.
ISO 27001
INFORMATION SECURITY MANAGEMENT
UKAS MANAGEMENT SYSTEMS
0015

We were approved by NQA Certification Ltd as meeting the requirements of the ISO 27001:2022 information security management systems standard in December 2024.

Our registration is valid until December 2027, when it will be renewed.

Cybersecurity controls

We have implemented several market-leading cybersecurity threat management solutions

Data protection and encryption: We implement stringent data protection measures to ensure the security of sensitive information throughout its lifecycle. All data is encrypted at rest and in transit using AES-256 and TLS 1.2+, with encryption keys securely managed in a FIPS 140-2 compliant Key Management System (KMS). We have Data Loss Prevention (DLP) technology in place to prevent unauthorised data access or sharing, while threat intelligence capabilities extend protection by proactively monitoring for leaked credentials and exposed data on the dark web.

Resilient cloud infrastructure: Shieldpay's multi-cloud architecture, built on AWS and GCP, ensures scalability, security, and operational resilience. Our services are hosted across multiple availability zones, providing high availability, redundancy, and fault tolerance. To safeguard against service disruptions, we deploy automated scaling, DDoS mitigation, and Web Application Firewall (WAF) protection. Additionally, physical security measures at our cloud data centres include restricted access, biometric authentication, and 24/7 surveillance, ensuring a secure foundation for our platform.

Threat detection and intrusion prevention: Our platform is protected by 24/7 security monitoring, real-time threat detection, and a dedicated security team. We use Extended Detection and Response (XDR) to provide advanced threat visibility across endpoints, networks, and cloud environments, enabling proactive threat hunting and rapid mitigation. Intrusion Detection and Prevention Systems (IDS/IPS) actively monitor and block suspicious activity. Embedded monitoring mechanisms, such as canary tokens, enhance our ability to detect unauthorised access.

Access and identity management: We enforce strict role-based access controls (RBAC) to ensure users have only the access they need. Single Sign-On (SSO) and Multi-Factor Authentication (MFA) strengthen authentication, with phishing-resistant FIDO2 hardware security keys deployed for privileged accounts. We leverage a centralised platform to manage identities, access, and user lifecycles seamlessly. Supported by robust Joiner-Mover-Leaver (JML) processes, this platform ensures consistent control and oversight. Conditional access policies authenticate both users and corporate devices, allowing only trusted endpoints to access critical systems. Regular access reviews, detailed logging, and anomaly detection further enhance security and maintain oversight.

Secure software development: We integrate security into every stage of the Software Development Lifecycle (SDLC) to ensure a resilient and secure platform. Our development process includes static and dynamic code analysis, secrets scanning, and mandatory peer code reviews to detect vulnerabilities early. Supply chain security is embedded into our CI/CD pipelines, with automated dependency scanning and integrity checks ensuring that only approved and secure components are included in releases. Regular penetration testing and threat modelling further strengthen our defences, ensuring every deployment meets the highest security standards.

Third party and supply chain security: Shieldpay maintains a rigorous third-party risk management program, ensuring that all vendors, suppliers, and partners adhere to our security and compliance standards. This includes thorough due diligence, ongoing monitoring, and security assessments to identify potential risks. Contractual agreements enforce strict security controls for all third-party engagements.

Employee screening, training and awareness: We conduct comprehensive pre-employment screening for all employees to ensure trust and compliance. Our team undergoes ongoing security training and awareness programs tailored to each level of the business, including phishing simulations, social engineering training, and regulatory compliance workshops. 'Game days' are used to simulate a failure or event to test our systems, processes, and team responses. By fostering a culture of security, we empower our employees to actively contribute to the protection of our platform.

Penetration testing and continuous vulnerability management: Regular penetration testing is conducted in collaboration with CREST-accredited security firms and utilises CBEST to simulate real-world attack scenarios and uncover vulnerabilities. Alongside penetration testing, advanced tooling is employed for automated scanning and threat intelligence-led attack surface monitoring, providing proactive risk detection. The continuous vulnerability management program ensures that critical security patches and updates are applied promptly, minimising the attack surface and enhancing overall security.

Incident response and business continuity: Our dedicated 24/7 incident response team follows predefined security protocols to rapidly contain and mitigate security incidents. Incident response plans are continuously tested to ensure swift remediation with minimal impact. Our business continuity and disaster recovery programs are regularly assessed to guarantee operational resilience in the event of disruptions.

Security logging and auditing: Shieldpay is committed to transparency and continuous security improvement. Our Security Information and Event Management (SIEM) system provides real-time monitoring, logging, and analysis of security events across all systems. Regular internal and external security audits validate our compliance with industry best practices and regulatory standards

Fraud prevention and threat intelligence: Our advanced fraud prevention tools actively monitor for suspicious activities, such as unusual transaction patterns, ensuring potential threats are identified and mitigated early. Complementing this, we integrate proactive threat intelligence into our security framework, continuously monitoring the dark web, deep web, and public internet for leaked credentials, data exposure, phishing domains, and brand impersonation attempts.

Insurance

We maintain a comprehensive insurance program, working with leading brokers in the Financial Services sector to ensure that we have appropriate coverage for all insurable risks relating to our business.

General office policies

We maintain the following general insurance policies:

Policy	Sum assured	Cover basis	Insurer(s)	Ratings
Employers' Liability	£10 million	Per claim	Aviva Insurance Ltd	AA- (S&P) AA3 (Moody's) AA- (Fitch) A+ (AM Best)
Public Liability	£5 million	Per claim		
Product Liability	£5 million	Per claim and in aggregate		

Professional policies

We maintain the following professional insurance policies in connection with our services on a worldwide basis:

Policy	Sum assured	Cover basis	Insurer(s)	Ratings
Professional indemnity	£100 million	Aggregate	Mosaic Sompo Hamilton CNA Allied World Company	A+/AA- (AMB, Fitch) A+ (S&P, AMB) A (AMB) A+ (Fitch) A+/A (S&P, AMB)
Crime	£100 million	Aggregate		
Cyber	£10 million	Aggregate	Mosaic	A+/AA- (AMB, Fitch)

Professional indemnity

Our Professional Indemnity policy covers claims resulting from:

- the provision of financial, payment or other professional services performed by us (including administrative and other operational services supporting the provision of those services); and
- the use of any technologies supplied by or on our behalf to support the provision of those services (including data processing, data and application hosting and network management).

Covered losses include any amount we become legally liable to pay resulting from any claim for compensation, damages or other relief, awards of costs, settlements, pre- and post- judgment interest and any amounts we are required to pay into any consumer redress fund.

Crime

Our Crime policy covers any direct financial loss (including loss of funds and interest on those funds) incurred by us or any third party for whom we hold and control funds, resulting from any fraudulent, dishonest, malicious, or criminal act or omission, no matter how or by whom perpetrated.

Crime also includes:

- cybersecurity breaches; and
- presentation of forged, fraudulently altered or fraudulently obtained documents in any format, where we have relied upon them;
- theft or dishonest retention of funds; and
- inability to recover funds misdirected or erroneously transferred to an account held at any financial institution.

Covered losses also include costs and expenses related to the verification, reconstitution or removal of data following a crime, the appointment of external specialists to determine the amount of any direct financial loss and claims preparation costs.

Cyber

Our Cyber policy covers claims resulting from:

- an actual or alleged cybersecurity breach causing any failure of, unauthorised access to, or unauthorised use of any part of, our technical infrastructure;
- an unplanned and unintentional outage of or interruption to all or part of our technical infrastructure;
- denial of service attacks;
- the receipt or transmission of malicious code;
- theft of passwords or other access credentials;
- theft, loss, or unauthorised disclosure of, personal data or confidential information that is under our care, custody or control;
- breach of data protection law; and
- failure by us to comply with our own privacy policies.

Covered losses also include costs and expenses related to any of the above, including forensic investigation costs, mitigation and remediation costs, legal advice, notification costs, identity monitoring and identity theft assistance, data recovery costs, hardware replacement costs and extortion costs (with the insurer's prior written consent).

Please note: The above represents a summary of our insurance policies. Insurance cover is subject to policy terms and conditions, excesses and exclusions.

Safeguarding

Overview

As an FCA-regulated payment institution, we are required to comply with strict requirements to protect 'relevant funds' received for the provision of our payment services. 'Relevant funds' means sums received from, or for the benefit of, a payer or payee for executing a payment transaction, and sums received from another payment service provider (such as a bank or another payment institution offering payment account services) on behalf of a payer or payee.

The Payment Services Regulation 2017 (**PSR**) permit us to safeguard funds by either holding the funds in a separate account which is segregated from our operational funds (the 'segregation method') or by covering the funds with an insurance policy or guarantee (the 'insurance method'). Shieldpay uses the segregation method.

Banking partners

The PSR permit us to hold relevant funds in safeguarded accounts with:

- an authorised credit institution, being a bank or other financial institution that has been granted permission to take deposits and grant credit;
- the Bank of England; or
- an authorised custodian authorised by the FCA or an equivalent EU regulator to safeguard and administer investments in secure and liquid assets.

The banking partners used by Shieldpay are:

We hold funds with Citibank, N.A., which is authorised by the PRA and regulated by the FCA as an authorised credit institution. Citi is a Tier 1 bank and investment bank which is rated as 'Stable' by the leading global credit and financial strength ratings agencies.

Clearbank Limited is a UK-based, tech-focused bank, which is authorised by the PRA and regulated by the FCA as an authorised credit institution. As an agency bank that holds its funds securely with the Bank of England, Clearbank does not have a traditional credit rating from the global credit and financial strength ratings agencies.

Blackrock is a leading investment manager and the world's largest asset manager. BlackRock Investment Management (UK) Limited is authorised and regulated by the FCA as an authorised custodian. Relevant funds are held within a recognised money market fund scheme which only deals in low-risk secure and liquid assets, specifically, government bonds and debt securities with short-term maturities. This fund is rated as 'Stable' by the leading global credit and financial strength ratings agencies.

Safeguarding procedure and audits

We have zero appetite for any material breaches of our safeguarding policy, including commingling of funds, non-completion of daily safeguarding reconciliations, reconciliation errors and discrepancies that cannot be resolved by the end of the business day, non-maintenance of designated safeguarding accounts, and non-escalation of safeguarding incidents.

Our safeguarding framework is audited annually by an independent firm of auditors. Our 2025 audit was assessed as 'Green' with an overall score of **99.88%** (2024: 90.98%). We take our obligations seriously and are committed to meeting and exceeding industry benchmarks to provide the highest level of trust and reliability for our clients.

Insolvency risk

Shieldpay is a regulated payment institution and not a bank, and as such, we do not have a traditional credit rating. However, as an authorised payment institution, we adhere to strict regulatory requirements set out by the FCA which includes:

- maintaining robust capital adequacy to ensure we have sufficient financial resources to support operations and protect our clients
- implementing strict liquidity management practices to ensure we can meet all obligations as they arise
- regularly undertaking audits and compliance checks to ensure our adherence to safeguarding and operational standards

'Relevant funds' held in safeguarded accounts are 'insolvency remote', meaning that in the event of Shieldpay's insolvency, relevant funds are ringfenced and do not form part of our assets for the purposes of meeting the claims of any creditors.

If Shieldpay's board resolves to enter into a solvent liquidation, it would execute a four-month wind-down plan, which would ensure that all relevant funds are returned to those persons entitled to them, or to another provider holding the necessary regulatory permissions, where appropriate.

If Shieldpay became insolvent, then the special administration process set out in the Payment and Electronic Money Institution Insolvency Regulations 2021 would apply. Following the appointment of a special administrator by the court, the special administration would take over the management of Shieldpay's business to achieve the objectives of the administration and ensure that all funds received and held by Shieldpay continue to remain safeguarded in accordance with existing safeguarding procedures. If it is determined by the special administrator that Shieldpay cannot be rescued through administration, or a plan cannot be agreed with our creditors, the company may be placed into liquidation with any relevant funds being returned to those persons entitled to them, or to another provider holding the necessary regulatory permissions, where appropriate.

Financial Services Compensation Scheme

The Financial Services Compensation Scheme (**FSCS**) is an independent, government-backed, scheme established to pay compensation if any eligible financial institutions fail. The amount of any compensation is capped at £120,000 per eligible person, per eligible financial institution.

Relevant funds held by Shieldpay with Citibank or Clearbank are within the scope of FSCS.