Information Security

The financial services sector continues to face increasingly sophisticated cybersecurity threats. As such, Funding Circle is committed to investing in the business and technical controls to help prevent, detect and respond to cybersecurity risk.

Funding Circle maintains information security controls that are designed and implemented to protect Funding Circle customers as well as staff data, information technology assets, and reputation through the preservation of:

- Data Confidentiality – Knowing and ensuring that information can be accessed only by those authorised to do so.

- Data Integrity – Knowing and ensuring that data are accurate and current and that they have not been deliberately or inadvertently modified from a previously approved version.

- Data Availability – Knowing and ensuring that data can always be accessed when required.

Funding Circle's Information Security framework is designed to specifically address legal and regulatory obligations and requirements that must be complied with. These requirements are based on a number of industry best practice frameworks including but not limited to NIST (National Institute of Standards and Technology) Framework and CIS (Center for Internet Security) Controls, which provide safeguards to mitigate risk and are also aligned to ISO270001. We keep to strict information security standards and regularly have internal and external audits of our security controls. Independently, we test the effectiveness of our security controls using specialists to perform penetration testing and 'Red Team' exercises.

Our Corporate Governance Framework oversees the management of information security risk in line with our risk appetite. We give quarterly reports to the Risk Committee and our Operational Resilience Strategy is reviewed by the Board of Directors yearly. Operational governance is provided across the Three Lines of Defence model, with continuous oversight and monitoring, including in respect of incidents and responses, identification and remediation of vulnerabilities, and redress of internal and external audit findings and business change management. This allows us to act quickly if we need to strengthen due to industry/regulatory requirements or in response to new security threats.

All suppliers or third parties that require access to Funding Circle's information systems as part of the service that they provide or if they handle data on behalf of Funding Circle, must comply with all Information Security Policies. For more information see: Supplier Assurance.

All employees receive training at onboarding as well as periodic and refresher training to ensure they have sufficient awareness and understanding of information security.