# The 12 security-related questions firms should be asking their platform partner

## Risk management

### 1 How do you ensure that client data is protected and your systems are secure?

At Fidelity, protecting client data and our systems is of the highest priority. We have a comprehensive information security framework in place which defines the level of protection required to mitigate the risks associated with accidental or unauthorised use, modification or destruction of information. It also sets out best practice for ensuring the confidentiality, availability and integrity of our information and systems.

Our security measures include employing a dedicated team whose core focus is early cyber breach detection and response. We also undertake email monitoring in order to prevent data leakage. We believe the protection measures we have in place are among the strongest in the industry.

### 2 How robust is your Information Security Management System (ISMS)?

As a global organisation, we are aligned with the internationally-recognised ISO family of information security standards. They provide assurance over the security of data by outlining a systematic approach to managing sensitive information. Our accreditations include ISO27001 (Information Security Management) and ISO200001 (Information Technology Service Management).

### 3 What controls and risk-assessments do you place on third parties?

We adopt very high information security standards and it is vital that our partners, suppliers and third party agents respect the same levels of security, integrity and approach to risk that we do. We have an established security framework which controls and assures the organisational and technical security controls of our suppliers before, during and at the end of an engagement.

This framework incorporates policies and procedures applicable to all colleagues engaged with suppliers, contractual requirements (including Non-Disclosure Agreements, confidentiality agreements and Information Security contract schedules) and a programme of robust risk-based supplier information security assessments, conducted at the outset of a new relationship and throughout the lifetime of a contract.

# Network security

## 4 How are your network and servers protected against external threats and attacks?

We use multiple levels of security including web application firewalls, vulnerability scanning applications, anti-virus software, code reviews, pen testing and malware detection and protection. Intrusion Prevention Systems (IPS) are deployed throughout our network and are monitored by our dedicated Cyber Defence Operations team.

# Incident management

## 5 How do you respond to a cybersecurity incident?

We operate a Major Incident Management (MIM) process which defines our approach for the way high-impact incidents are handled. We also run an Incident Management operation which is designed to tackle and resolve cybersecurity issues using a pre-defined, risk-based rating scheme. This process includes a post-incident review where lessons learned from previous incidents are identified, managed and implemented into future security incident plans and procedures.

## 6 What data recovery, business continuity and disaster recovery plans do you have?

Regular data backups are performed, secured and saved in disk storage units housed in secure Fidelity-managed data centres. We adopt various business continuity recovery strategies covering the loss of people, systems and site. Disaster recovery strategies include alternate-site working and remote-working plans. Business continuity plans are in place for all business areas and regular tests are conducted including disaster simulation exercises and emergency management drills.

# Managing user privileges

## 7 Are staff user privileges and data access rights controlled?

We operate a role-based access control model which governs staff access to data. Access-provisioning ensures employees are permitted to have only one role at a time and access is reviewed on a regular basis. Access is revoked upon termination of employment for any member of staff within 24 hours of leaving the company.

## 8 What security measures are in place in relation to staff working from home (or remotely) and using removable media?

We only provide remote access to staff who have completed approved requests and passed our security requirements. It is protected by two-factor authentication and is provided via a secure Virtual Private Network (VPN) connection. The ability to copy or print data is disabled for all staff and rights to read or write to removable devices are blocked as standard.

# Staff checks and education

## 9 How do you ensure staff are not a security risk?

We follow industry best practice for the screening of prospective employees, including, where applicable:

- Identity checks (using government issued ID).
- Address check
- Right to work
- Criminal history
- Employment background
- Education and certification verification
- Financial checks

All staff members go through a comprehensive programme of security training and awareness, which begins on the first day of employment and before access to our systems and information. There are mandatory annual information security training modules and campaigns on a variety of topical security issues.

# Fraud

## 10 How do you manage the risks associated with fraudulent email instructions?

We acknowledge the risks that email account compromise poses and understand that this is a common enabler of fraud. We aim to protect both financial advisers and their clients against these risks by applying additional layers of protection to both identify and prevent fraud in this area. In higher-risk transactions, we proactively contact advisers, reminding them of the risks and offering preventative advice in relation to both the matter at hand as well as future scenarios.

## 11 How do you ensure a payment instruction is genuine?

We operate a strong control environment and have a number of processes in place to prevent fraudulent activity. Ensuring that payment destinations are genuine is one such measure and, as a result, all new bank account details are subject to a robust verification process. This procedure is managed by a dedicated team of staff who are able to identify potential signs of fraud, ensuring the legitimacy of any given instruction and preventing fraudulent withdrawals from taking place. Much of the activity is conducted behind the scenes, minimising the impact on advisers and their clients.

## 12 Are you a member of Cifas, the UK's fraud prevention agency?

Yes, we are. Cifas works closely with UK law enforcement partners and membership provides valuable benefits. For example, we have access to the National Fraud Database and a wealth of data on thousands of instances of fraudulent conduct. This helps firms in the UK to prevent over £1 billion of losses to fraud every year. Similarly, access to the Internal Fraud Database prevents dishonest individuals and organised criminals from joining the company.

FundsNetwork

Fidelity™ INTERNATIONAL



UKM0819/24424/SSO/0820