



FINANCE & TECHNOLOGY RESEARCH CENTRE

Email Encryption & Secure Communication

Adviser business requirements for email encryption services

August 2009

Contact Details

Finance & Technology
Research Centre

T: 020 7659 2345

Ian McKenna
Director

E: ian.mckenna@ftrc.co.uk

Poppy Morgan
Research Consultant

E: poppy.morgan@ftrc.co.uk

Samantha Smith
Head of Marketing & Admin
E: samantha.smith@ftrc.co.uk

Email Encryption – Background & Objectives

Advisers are beginning to investigate email encryption, and other secure communication solutions for their businesses, as a response to calls from the FSA to tighten up on data security practices. A number of “off the shelf” solutions are currently available, however these have not been designed to specifically meet adviser business requirements.

F&TRC are conducting a research project which will document adviser requirements for an email encryption solution, with the findings being published in August 2009. The report will:

- Assist product provider understanding of adviser requirements and the solutions which will be meet these needs
- Define a set of requirements against which providers can assess their existing email encryption solutions before deciding whether these can subsequently be re-used with advisers
- Deliver guidance to adviser businesses seeking to adopt/or review an existing email encryption solution



F&TRC Credentials for this project:

- 👍 F&TRC have excellent working relationships with a wide range of networks and national adviser firms and also support groups
- 👍 We have a detailed understanding of the different operating structures within adviser firms, covering a wide range of approaches including (but not limited to):
 - Sole traders', small directly authorised network/support group members, medium sized regional firms, large scale national firms
 - Centralised admin support v local admin support
 - Mandated technologies v self select technologies
 - Enforced business processes v own business process
 - Employed staff v self employed staff
- 👍 F&TRC consultancy staff have all worked within IFA businesses, we therefore have a dedicated understanding of how such firms operate

Contact Details

Finance & Technology
Research Centre

T: 020 7659 2345

Ian McKenna
Director

E: ian.mckenna@ftrc.co.uk

Poppy Morgan
Research Consultant

E: poppy.morgan@ftrc.co.uk

Samantha Smith
Head of Marketing & Admin
E: samantha.smith@ftrc.co.uk

Project Deliverables

Overview of the different users of email and the nature of email communications being sent

Including: Identifying the main stakeholders

Highlighting situations where advisers are likely to regularly breach the Data Protection Act



Understand the complexity of the email trail

Including: Documenting scenarios detailing how emails are passed between different parties and what issues this could present to an email encryption service



Identifying the different types of devices advisers use to send/receive emails

Including: Adviser requirements for each device

Issues an email encryption service may need to consider



Document the issues advisers will need to consider and obtain answers to, prior to selecting a solution vendor

Including: Documenting the key challenges and issues an email encryption service will need to address with its target market

Production of a public domain document, designed to assist advisers to understand the questions they need to put to any email encryption vendor, prior to adopting a service



Assisting firms to validate whether an existing email encryption solution can be re-deployed across advisers

Including: List of requirements that any email encryption service will need to meet in order for it to be effective when dealing with adviser businesses



Table of Contents (1)

- Background
- Project Scope & Deliverables
- Methodology & Approach
- FSA & ICO
- Data Protection Act (DPA)
- Financial implications of breaching DPA
- Taking regulatory responsibility
- Scale & implications of current breaches
- Understanding the breadth of email usage in adviser firms
- Where are DPA breaches taking place?
 - Leads – how do advisers obtain these?
 - Fact find – how do advisers gather this information?
 - Illustrations – how do advisers & Providers communicate?
 - Suitability letter – how do advisers send this information on?
 - Applications – how do advisers and providers exchange data
 - Valuations – how do advisers obtain this data from Providers?
 - Aggregated statements – how do advisers send this information on to clients?
- Different advisers, different issues for Providers?
- Understanding different distributor models
- Overview of how different advisers approach technology
 - Adviser technology – the “Corporate” approach
 - Adviser technology – the “Guided” approach
 - Adviser technology – the “Individual” approach

Understanding the breadth of email usage in adviser firms

- Email communication is being used by adviser firms of all shapes and sizes.
- It has allowed firms to increase the speed at which information can be communicated between parties internal to the adviser business and those who are external to the business.
- Many firms are now starting to see an increase in client demand for email communication therefore the use of such services is likely to intensify.
- Information exchanged falls into 3 broad categories:
 - Non personal/sensitive i.e. generic information, will not include anything about the client.
 - Personal client information i.e. details that are public information e.g. name, date of birth.

“Should we use email? Absolutely, it is the most flexible and cost effective way to communicate.”

Understanding different distributor models

Key differences	National	Network	Support Group	Medium/Small IFA firm
Responsibility	<ul style="list-style-type: none"> • Adviser firm will have regulatory responsibility for its advisers. • Adviser firm will have responsibility for all directly employed staff. • Where individuals are employed by the adviser the adviser firm will be liable for any actions taken affect its customers. 	<ul style="list-style-type: none"> • Network will have regulatory responsibility for its advisers and any staff it directly employs. • Appointed representative will have responsibility for any directly employed staff as will the Network. 	<ul style="list-style-type: none"> • Support Group has no regulatory responsibility for its advisers or any staff the advisers directly employ. • Regulatory responsibility rests with the directly authorised firm. • Support Group will have responsibility for any staff they directly employ. 	<ul style="list-style-type: none"> • Adviser who is directly authorised (DA) will be responsible for managing all aspects of business risk. • Adviser who is an appointed representative (AR) the responsibility is likely to fall upon the firm adviser is appointed to.
People	<ul style="list-style-type: none"> • Advisers will be either employed, or may be self-employed. • Head office and staff will be an adviser firm, no individuals may be employed by the adviser firm. 	<ul style="list-style-type: none"> • Advisers will be self-employed and will be 	<ul style="list-style-type: none"> • Advisers will be self-employed and directly 	<ul style="list-style-type: none"> • Advisers will be self-employed.

Suitability letter - how do advisers send this information on?

Again, this process highlights the need for advisers to put in place secure communication mechanism if choosing to send clients suitability letters via email.

- A typical suitability letter will contain information such as:
 - Clients name
 - Clients address
 - Details of clients family (i.e. spouse and dependants including names and ages.
 - Details of clients financial objectives (i.e. savings, protection etc.
 - Details of clients existing assets and plans, may or may not include policy number information though the letter is likely to state how much these are worth/contributions being made.
 - Details of agreed actions.
- Whilst clients may have a preference to receive such letters via email advisers need to consider the risk (to the client and to their business) of communicating with them in this manner.

Adviser likely to send letter in the post although client could request it sent via email.

Suitability letters will contain information about the clients needs and goals, existing assets and agreed actions. There is sufficient information in this document to constitute a breach of DPA if sent via insecure email.

Table of Contents (2)

- Advisers and secure communication – state of preparedness
- Rules based encryption
- Different adviser approaches to securing communication
- Multiple solutions, multiple issues for advisers?
 - Servers
 - Hardware/Software
 - Email application
 - Mobile devices
 - Interoperability
 - Encryption keys
 - Storage & archive
 - Retrieving emails in the short term
 - Retrieving emails in the longer term
 - Support
- Meeting adviser request for information
- Due Diligence for email encryption
- “Islands” of security
- Email encryption – right tool for the job?
- What is an “industry” solution?
- Reusing what’s already in place
- How do existing solutions compare & exploring other solutions
- Secure communication – a possible B2B model?
- Taking a look at other sectors
- Key conclusions

Advisers and secure communication - state of preparedness

Journey	Fully compliant	Partially compliant	Careful	Careless
How many	<ul style="list-style-type: none"> FSTRIC research has found no firms that would fit into this category yet. 	<ul style="list-style-type: none"> Only truly a small number of firms who can claim to be at this stage. Achieving compliance is a major priority though will still be some way from this. Would expect this group to be compliant sometime 2010. 	<ul style="list-style-type: none"> Growing number of adviser firms appearing in this category. Suggests they are taking their obligations under the DFA seriously. However, have only just embarked on a journey to achieve compliance. 	<ul style="list-style-type: none"> Majority of adviser fall into the “careless” category. These will typically be the small-medium sized firms however, there are, surprisingly, some sizeable organisations who also fall into this category. Advisers will be breaching DFA on a regular basis. These firms are an accident

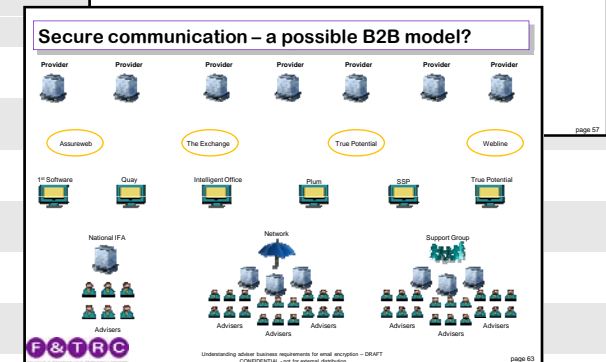
Due diligence for email encryption

Registration	<ul style="list-style-type: none"> What is understood about this organisation i.e. what is their standing within their community?
Ownership	<ul style="list-style-type: none"> Who owns the organisation?
Location	<ul style="list-style-type: none"> Which country are they based out of? Do they have local offices i.e. are they based out of the UK? If so, where?
Longevity	<ul style="list-style-type: none"> How long have they been operating for?
Specialists	<ul style="list-style-type: none"> What is the main area of expertise i.e. is it email encryption or do they offer a wider range of services which this is part of?
Host country for solution	<ul style="list-style-type: none"> Where are servers/databases held e.g. US, UK, EU, Asia etc?
Staff vetting	<ul style="list-style-type: none"> Do they undertake staff vetting procedures?
Standards compliance	<ul style="list-style-type: none"> Which of the following standards does the solution vendor comply with:

“Islands” of security

- Comment has been made by some advisers has been that a firms information security policy should be seen as an “island”.
- Each “island” is responsible for its own processes and data and should not seek to impose their way of working on other parties.
- Advisers have stated that whilst they are keen to receive information in a secure format from Product Providers they are concerned that Product Providers will push out a solution that will have to come into their island rather than step just at the door.

“Look at it as ‘islands of security’ – each island has their own processes and responsible for their own data but, each has to find a way of passing data to each other.”



Contact Details

Finance & Technology
Research Centre

T: 020 7659 2345

Ian McKenna
Director

E: ian.mckenna@ftrc.co.uk

Poppy Morgan
Research Consultant

E: poppy.morgan@ftrc.co.uk

Samantha Smith
Head of Marketing & Admin
E: samantha.smith@ftrc.co.uk

Adviser Participants



bankhall

Bluefin



 FosterDenovo

Park Row

Openwork

sesame

 **SimplyBiz**



SKIPTON FINANCIAL SERVICES

threesixty

Pre Publication Price (for orders received before 14th August 2009):

£ 6,500 + VAT

Post Publication Price:

£ 8,000 + VAT