

Email – the best channel for Offshore Banking?

The challenges facing Offshore Banking

Customers can't just pop into the local branch of an offshore bank to transact business and this brings a range of challenges in how to conduct business both securely and efficiently while operating at a distance.

Banking has changed significantly in recent years with a rapid growth in telephone and internet channels to supplement the traditional branch - which itself is evolving from a processing centre to sales outlet. These changes, while well placed for mainstream retail banking are often ill-suited for the more specialised needs of the offshore customer.

A typical offshore bank is smaller, has a mix of personal (usually wealthy) clients and institutions such as insurance companies and fund management firms who are managing monies for their clients. Often, their small size means that they don't have the budget available to invest in significant operational and technical change which larger banks can achieve.

Typically instructions are received by letter, fax or telephone and although some offshore banks have websites these are often not suitable for transactions either due to a lack of security, the need to have multiple parties confirm transactions or it is not designed to manage the complexity and range of requests received. As a result offshore banks have a high proportion of requests by fax and letter, but this means that instructions are often received in different formats making processing more expensive and prone to error.

Telephony, which through the use of call centres and mobile technology has itself changed significantly in recent years, has its own challenges with how to positively identify customers and what hours to operate given that the customer is often located in a different time zone.

There are also challenges to banks and their clients corresponding by post. Postal interception in some countries is a very real problem and has resulted in significant fraud.

Email has quickly grown to be the most important business communication medium - it is cheap, efficient, convenient and ubiquitous. However, the sending of unencrypted emails over the internet represents a major threat to security and confidentiality. It's the electronic equivalent of sending a postcard – potentially, anybody can read it – and as a result the use of email has been restricted or even prohibited.

There are other problems too. How can you sign an instruction to a bank and send it by email? What happens when more than one signature is required?

So what is needed?

The technology now exists to make email a practical customer service proposition and transport mechanism for transacting banking business. Customers are used to using email and are often surprised when a bank refuses to use it – they are generally unaware of the security challenges.

Most organisations have Microsoft Exchange or Lotus Notes as email systems but the key is in ensuring that the email system deployed can both cope with the potential volume and nature of emails in an appropriate manner. This includes having suitable email routing and retention strategies in place so that customer service is maintained during staff absence. It also means ensuring emails can be found months or years later should it be necessary.

Email recipients have a broader choice of email client from Outlook, Apple Mail and Thunderbird to web-based systems such as Yahoo and Hotmail. Email communication with customers must be able to work with these different systems, ideally without requiring any additional software on the customer's PC.

Email Encryption

When a user sends an email it appears to go directly from the sender to the recipient. In reality it may transfer via a number of different servers which, due to the way the Internet works, can be anywhere. Therefore, whenever an email is sent, it is as if you have sent the message on a postcard. Anyone with the tools and desire could theoretically intercept and read or alter it. This means that standard email is an inappropriate medium to use when personal or confidential data needs to be communicated.

The principles of protecting information are enshrined in Sarbanes-Oxley, the Data Protection Act, Basle II and other legislation covering the UK, the USA and Europe. It is incumbent on organisations to take suitable care to protect confidential data and this means that emails should be encrypted between the parties.

The solution should permit an email from a bank to be sent encrypted to the desktop of the recipient. If the recipient is a company it may be acceptable to them to encrypt just to their email gateway. Ideally, the decision to encrypt can be automated, based on criteria such as recipient email address or message content, removing operator error from the process. Of course, there will be situations where the system should also allow manual over-ride of automated decisions.

It should be possible to send encrypted email to any email address and ideally using any of a wide range of encryption methodologies - the choice being partially related to the sophistication of the recipient and whether they have invested in solutions such as PKI or PGP. Again, as far as the email author is concerned the actual encryption methodology deployed shouldn't matter - what does is that the message is sent securely and that the recipient can decrypt and read it.

At its simplest all a recipient needs to do is register their email address and a password and the encrypted message can be sent to them alternatively they could be pre-registered by the bank and an initial password sent by post or even SMS.

There should be no need for the recipient to download any software. It is now possible to send messages securely using encrypted PDFs - so that there is no additional client software to install with all the support challenges that software installation can bring.

Clicking on the PDF attachment to open it will cause a box to appear requesting the user's password – correct entry of the password will decrypt the message.

Secure Response

There are occasions when you will want to be able to receive a secure response from a customer – this could be a completed application form or a free-format reply to the email that you have sent.

Any decent secure email system must permit the easy response to a message without impacting on the integrity of the communication – and this needs to be workable for any recipient and be independent of any software that they might have installed.

Hiding a Sender's Identity

Some customers might be keen to use email but are concerned that sending an email address, which would have the domain name for the offshore bank as part of it, might leave their banking relationship exposed even though the content of the message is encrypted.

It is possible to further protect a customer by hiding the identity of the sender's email address and translating it to something benign when received by the customer. As a result even the customer's ISP would not be able to tell that the email had originated at a bank, e.g. RelationshipManager@offshorebank.com translates to 123456@benigndomain.com

A response by the customer to the apparent sending address would be translated back and routed to the correct relationship manager.

Intelligent Email Routing

A further problem with email is how does an organisation differentiate between unsolicited emails and spam and a request from a customer to execute a specific instruction? And what about differentiating between different types of customer request?

It is possible to analyse incoming emails and their attachments and route them to the most appropriate customer service department. This can be done automatically with no manual intervention.

At the heart of this technology is the ability to examine a message or document and identify the context. The software then determines how the message should be categorised, who should see it and what other material it should be linked to. This capability can also be used to filter unsolicited emails prior to their entry into the organisation. The system could also be used for automated email response.

Identity Verification

e-Solutions, in partnership with Equifax, provide an identity verification service which permits an individual's identity to be confirmed at a distance and in real time, without the inconvenience of physically producing a passport, a driving licence etc. Once identity has been confirmed, then a digital certificate can be issued, which can be used to digitally sign emails and documents and for email encryption.

The certificates are tScheme accredited – Equifax was the first provider in the UK of authenticated certificates approved for government use. The system can be used to confirm the online identity of residents in the UK.

Digital Certificates and Signatures

In addition to the uses above, a digital signature contained within a certificate will confirm that the document received is identical to the one sent – that it has not been altered or tampered with in anyway.

Email Archiving and Retrieval

Although it is good business practice to back-up email systems, and most companies have processes in place, this is not the same as archiving email.

Backup files are generally designed to restore lost data after a major failure and as such are difficult to search for individual items. Depending on how the backup cycle operates, it might also be possible for emails to be deleted by a user and making them irretrievable (which could breach regulations).

Archiving is different in that it operates separately to the standard backup. Copies of email are taken and held independently from your current email server.

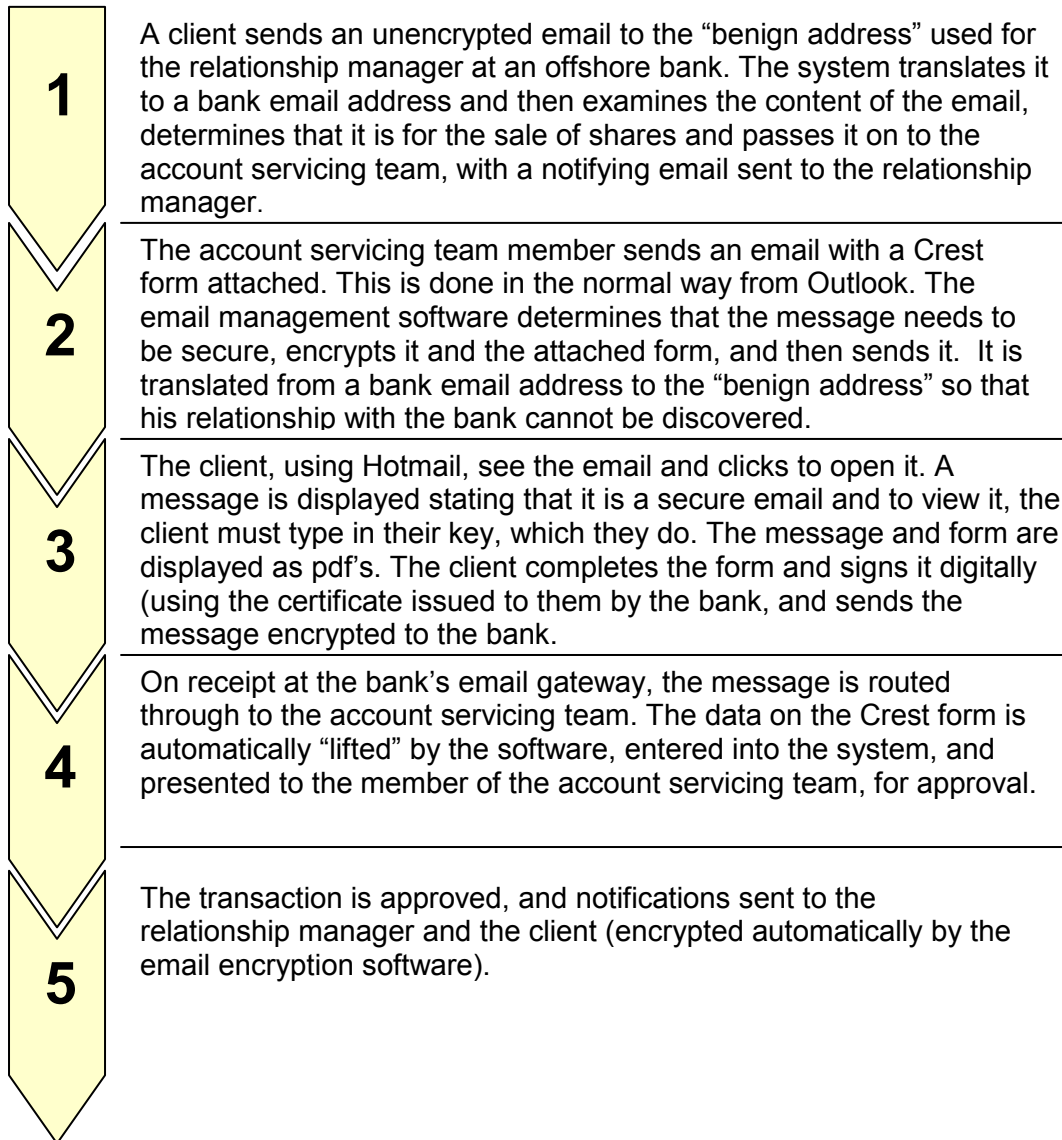
Once email has been captured in an archive it is possible to undertake robust analysis to cover:

- Policy violation reporting.
- Abuse management - suspicious or inappropriate email being sent.
- Personal usage by staff against agreed guidelines.
- Forensic investigation - permitting access by managers without recourse to IT.
- Compliance - providing an audit trail for FSA, Sarbanes-Oxley, Data Protection and other regulatory and legislative requirements.
- Volume analysis - understanding where emails are being sent to and received from.
- Proof of a transaction request and receipt of notification.

It all needs to hang together

Email has the capability to become the channel of choice for the offshore banking community – but only if it provides a comprehensive, secure and easy-to-use service. This means that all the components described above have a role to play – and it's important that they work together in an integrated and cohesive way.

A typical transaction in an email-enabled customer contact centre



**Process
completed**

The benefits of using email

Email has a lot going for it – that's why it's so widely used. The main benefits for an offshore bank in using email to communicate with customers are:

- It's available 24 x 7.
- It's geographic reach.
- The audit trail.
- Improved customer service.
- Convenience.
- Customer acceptance, understanding and use.
- Reduced operational costs for offshore banks.

Email management and encryption allows a bank to extend the use of email to new functional areas – it's only a matter of time before customer contact processes are re-engineered to take advantage of it.

Further information Please contact us for more detailed information on our range of email management solutions and how they can be tailored to meet your specific business requirements.



Technology Solutions for Business

e-Solutions and Services UK Ltd
Upper Linbrook Farm
Needwood
Burton-upon-Trent
Staffs DE13 9PF

Phone: 0870 855 0631
Fax: 0870 855 0639

Email: enquiries@e-solutions.uk.com
Web: www.e-solutions.uk.com
