

## EMAIL AS EVIDENCE

### 12 STEPS TO ENSURING GOOD EVIDENTIAL QUALITY OF EMAIL



Today's litigious and regulatory environments mean organizations are obligated to electronically store information to support discovery and disclosure requests. Organizations that archive email in a 'fractured' environment risk losing control and may struggle to produce evidential-quality email evidence.

## CONTENTS

Audience and remit	2
Mimecast foreword	3
Executive summary	4
The legal obligation to give disclosure of electronic documents	5
Fragmented email environments	8
Authenticity in a fractured environment	11
Litigation that is commonly concerned with email	13
12 steps to ensuring good evidential quality of email	14

## AUDIENCE AND REMIT

The intended audience for this White Paper includes corporate counsel, IT management, compliance managers and others concerned with the management of email, although legal experience and knowledge is not assumed.

The remit is the writer's experiences as a litigator and advocate.

## THE AUTHOR

Stewart Room is a partner at European law firm Field Fisher Waterhouse LLP, where he specializes in the contentious aspects of privacy, information and technology law. He is dual-qualified as barrister and solicitor, with over 16 years' experience as a litigator and advocate.

He is the President of the National Association of Data Protection Officers, author of 'Data Protection and Compliance in Context' (2006), 'Email: Law, Practice and Compliance' (2008) and is rated as a leader in the field of data protection and privacy by the legal directory Chambers UK. His clients include BP, BBC, Marks & Spencer, Nestle, RSA, Symantec and Unicef.

 Field Fisher Waterhouse



# MIMECAST FOREWORD – EMAIL AS EVIDENCE

DR JAMES BLAKE, CHIEF PRODUCT STRATEGIST



Infrastructures of potentially dozens of servers have built up around corporate email systems to provide better governance, reduced risk and improved legislative compliance – anti-virus, anti-spam, attachment handling, encryption, disclaimers, archiving and hot-standby mail servers to name a few.

These disparate email environments provide a fragmented approach to applying email policy and lack overall visibility of email threats. This traditional approach also impacts the quality of the evidence that can be provided by creating barriers to extracting information quickly and in a relevant format.

Mimecast's approach has always been to build a single web-based email management platform, rather than creating standalone technologies and attempt to integrate them. The entire Mimecast service abstracts the user from the underlying technologies involved and instead provides a service that offers strong chains-of-custody, constant availability, sub-second discovery and an infinite storage capability.

## EXECUTIVE SUMMARY

Litigants in this country are required by law to give disclosure of electronic documents. This process is often called 'e-discovery'. The obligations are found in the Civil Procedures Rules (CPR). Litigants that fail to give proper disclosure are exposed to serious sanctions.

The law takes disclosure seriously because it is one of the cornerstones of civil justice systems. The law generally prefers a 'cards-up' approach to the resolution of disputes, albeit with exceptions. However, while the spirit and intention of the rules cannot be derided, the fact remains that the process of e-discovery can be an onerous obligation, particularly where the litigant and the lawyer are working in a 'fractured' environment and particularly where emails are involved.

The nature of a 'fractured' environment is one where electronic documents are not properly managed resulting in a loss of control. A fractured environment causes electronic documents to be used and stored erratically, the provenance of electronic documents might be unclear, rules on retention and deletion might be user-defined rather than organization-defined, and there might be problems of considerable duplication.

A fractured environment is detrimental to electronic documents and if litigation touches such an environment the e-discovery process is inevitably more complex, more time-consuming and more expensive than in cases affecting organizations with properly managed data systems. Moreover, the litigation may be less efficient, in the sense that important documents can be overlooked, which can weaken cases and, ultimately, lead to failure when success might otherwise have been more likely and the more just result. Another risk of a fractured environment is that legally privileged documents could be disclosed by mistake. Even worse a fractured environment might result in the withholding of documents that assist the other side, which can give rise to accusations of concealment, which is a very serious charge.

Litigation is not the only reason why organizations should take control of their electronic documents; there are many regulations that require the long-term retention of documentary records and their production to regulators during regulatory proceedings and investigations. In a fractured environment, organizations run the risk of breaching these regulations.

This White Paper summarizes the author's experiences of litigating in fractured environments, particularly as they pertain to email. In light of these experiences, it is the author's opinion that potential litigants are always best advised to gain control of their email systems and because email is a technological issue, this requires technological solutions. This White Paper also identifies some key regulations that require the retention of documentary records and their production to regulators.

## THE LEGAL OBLIGATION TO GIVE DISCLOSURE OF ELECTRONIC DOCUMENTS IN LITIGATION ('E-DISCOVERY') – AN INTERNATIONAL PERSPECTIVE

The primary obligation to give disclosure is contained in Part 31 of the CPR and it mirrors closely the corresponding obligation in the United States, which can be found in Rule 26 of the Federal Rules of Civil Procedure (FRCP). When the CPR and FRCP are compared and contrasted it will be found that the similarities greatly outweigh the differences. Which should not be surprising bearing in mind the shared ancestry of these legal regimes, the common law approach of both jurisdictions, the adversarial approach of both jurisdictions, the shared language, the very close social, political, economic relationships and ties and the increasingly international flavor of litigation.

Indeed, the close connections and cross-pollination of ideas on e-discovery between the UK and the US is evidenced by the fact that the CPR's rules

on e-discovery were amended in 2005 in reaction to earlier work on e-discovery by the US organization, the Sedona Conference<sup>1</sup>.

The fact that the UK and the US have taken very similar lines on e-discovery is of more than mere academic interest. It tells organizations that e-discovery is an issue of international significance and in this environment of increasing globalization, where cross-border disputes are becoming common, it would be a brave – or foolish – organization that would choose to tolerate a fractured environment; the chances of electronic documents being called upon by courts and regulators are increasing exponentially and organizations need to adapt to handle this fact, particularly where they interact or do business with other organizations or individuals situated in other countries.



## CASE STUDY

In 2006 Morgan Stanley agreed to pay a \$15 million fine to the Securities and Exchange Commission (SEC), for repeatedly failing to produce emails during the course of investigations concerning share allocations in IPOs. The SEC's complaint said:

"From December 11, 2000 through to at least July 2005, Morgan Stanley failed to produce tens of thousands of emails sought by Commission subpoenas and other requests issued in the course of two Commission investigations: an investigation into Morgan Stanley's practices in allocating shares of stock in initial public offerings ('the IPO Investigation') and an investigation into conflicts of interest between the firm's research and investment banking practices ('the Research Analyst Investigation'). As a result, Morgan Stanley violated the provisions of the federal securities laws requiring Morgan Stanley, a regulated broker-dealer, to timely produce its records and documents to the Commission."

The Morgan Stanley case provides a salutary warning to organizations about the need to take emails seriously, for the purposes of records-keeping and for the purposes of regulatory investigations. Among other things the Morgan Stanley experience teaches organizations the following priorities for email:

- **During the course of regulatory investigations they should ensure diligent searching of archives.**
- **Any statements to regulators about the availability of email should be wholly accurate.**
- **Emails should be delivered up in a timely fashion.**
- **The introduction and implementation of an email archive is a high priority.**
- **Emails should be properly preserved, to avoid deliberate or accidental overwriting and deletion.**

But what is the relevance of this case for organizations in the UK? The answer is simple; first, this case reinforces the message that e-discovery is an international issue; second, there is plenty of evidence to show that US regulatory initiatives and approaches have impact and are followed in the UK, as illustrated by the increasingly interventionist approach of the Financial Services Authority, the UK equivalent of the SEC.

### E-discovery under the CPR

If Part 31 of the CPR is stripped down to its fundamentals, a clear, core obligation is discovered; a litigant is obliged to give disclosure of documents that they rely upon, or which undermine their case, or which assist the other side's case and if they fail to give proper disclosure of the final two categories of documents they can be compelled to do so by an order of the court.

This right/obligation approach is the hallmark of an adversarial legal system. Of course, in order to be effective on a day-to-day basis the right/obligation approach within the CPR is supported by considerable detail.

In summary, the core components of Part 31 of the CPR are:

- A litigant gives disclosure by stating that a document exists or has existed. For these purposes a document means anything in which information of any description is recorded, which includes electronic documents like email.
- The scope of the obligation is to give disclosure of relevant documents, which means documents on which the disclosing party relies, documents that adversely affect the disclosing party's case, documents that affect another party's case and documents that support another party's case.
- The documents that have to be disclosed are those that are or have been in the disclosing party's control. For these purposes a party has or has had a document in their control if it is or was in their physical possession, if they have or have had a right to possession of it or if they have or have had a right to inspect or take copies of it.
- When giving disclosure the disclosing party is required to make a 'reasonable search' for relevant documents and must sign a 'disclosure statement' explaining the extent of the search.
- The obligation to give disclosure is triggered by a court order. Once triggered the obligation continues for the life of the litigation. The parties are also under a duty to preserve relevant documents once litigation commences.

- The court can compel disclosure at any time, including against non-parties. The court can also order disclosure before litigation commences, if that would be fair.
- Documents that are protected by legal privilege, ones that form part of 'without prejudice' discussions and ones that incriminate the litigant of crimes are exempt from the obligation to give disclosure.

Part 31 of the CPR is supplemented by a Practice Direction, which gives detailed guidance on e-discovery, explaining that the obligation 'extends to electronic documents, including email and other electronic communications, word processed documents and databases. In addition to documents that are readily accessible from computer systems and other electronic devices and media, the definition covers those documents that are stored on servers and backup systems and electronic documents that have been 'deleted'. It also extends to additional information stored and associated with electronic documents known as metadata.'

E-discovery is clearly a serious and extensive obligation and it will be obvious that in a fractured environment it will be very difficult to comply.

### E-discovery under regulations

There are many laws and regulations that require organizations to keep electronic records, such as email. For example, under the Companies Act there is an obligation to keep full accounting records, under the Data Protection Act there is an obligation to keep personal data records, under the Freedom of Information Act there is an obligation to keep public sector records. Under financial services legislation such as the Financial Services and Markets Act and the Market in Financial Instruments Directive (MiFID) there is an obligation to keep records of financial transactions. In all of these examples there are obligations to give disclosure to regulators. As with the case of e-discovery in litigation a fractured environment acts as a barrier and impediment to the effective discharge of legal obligations under regulatory law, which can be punished with serious sanctions such as the imposition of fines, enforcement action and the imposition of onerous license conditions.

## FRAGMENTED EMAIL ENVIRONMENTS

Email forms one of a company's greatest assets – it is both a critical communications tool and a repository of historical business intelligence. Today, it provides supporting evidence during disputes with external parties and internal employees.

### A growing infrastructure

For a whole host of reasons, ancillary services have been built around email servers to provide risk mitigation from threats such as spam, malware, and data loss. In addition, other requirements for effective enforcement of email Acceptable Use Policies and legislative compliance have arisen. Over the past decade, vendors have reacted by providing dozens of technologies to solve the issues around email, such as email firewalls, email routing, denial of service protection, intrusion prevention systems, anti-spam, anti-virus, anti-phishing, attachment management, disclaimer management, email marketing, email storage management, high availability, archiving and managing discovery.

Almost all of the ancillary services deployed in an email infrastructure are designed to provide functionality in three broad areas: to increase internal governance; to mitigate risk and improve legislative compliance.

These solutions are typically deployed as they become necessary to adapt to new threats or regulatory requirements and build up organically

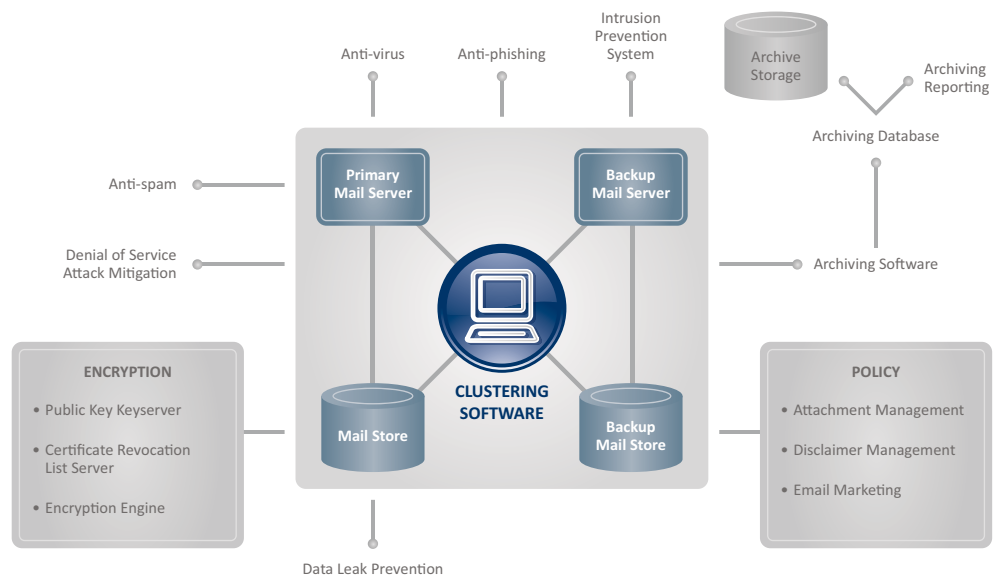
over time around the mail server. Each of these support services is typically provided by a separate point solution, each requiring maintenance and comes with its own provisioning and reporting interface.

### Managing multiple consoles

Each of these solutions will typically operate in isolation, independent of the actions that the other components are taking. Because each platform will log its actions into its own reporting environment, seeing the sum total of actions taken on a particular email may involve extensive aggregation and normalization of the logs from dozens of different servers. With a fragmented reporting infrastructure it is difficult to detect changing trends in email usage; identify anomalies; or even get a high-level snapshot of whether the level of risk involved with email is increasing or decreasing.

This fragmented environment results in islands of protection against specific threats but makes it very difficult to apply and enforce organization-wide policy. The fragmented environment also inhibits e-discovery – each email may have several different variants in existence within the receiving organizations due to multiple independent point solutions applying parts of the overall policy. Often the email recorded in an archive will be just one variant that may differ from the original email received.

### TRADITIONAL FRAGMENTED EMAIL ENVIRONMENT ARCHIVE



### Meeting the timetables for e-discovery in a fractured environment

One of the greatest problems for lawyers and organizations working in a fractured environment is how to comply with legal timetables for disclosure. It should not be underestimated that if electronic documents are not properly managed it can be extremely difficult, if not impossible, to comply with court and regulatory timetables.

When a litigant requires the court's or regulator's indulgence it usually creates a bad impression and can cause the other side to scent blood. Being on the back foot in litigation and regulatory proceedings should always be avoided.

Attorneys who are good litigators will always strive to put their clients in control, because it is from a platform of control that cases are won.

As far as emails are concerned, the problems associated with a fractured environment increase by a large order of magnitude. Part of the essence of email is its ability to reproduce, replicate and spread. Should an organization find themselves in a position of having to chase up and track down emails, they will be deflected from much more profitable endeavors within the proceedings, such as putting pressure on the other side!

## CASE STUDY

In the case of *Harper v. Information Commissioner*, litigation under the Freedom of Information Act, the Information Tribunal held that in appropriate cases the obligation to give disclosure of public sector information could extend to deleted electronic documents. The Tribunal said:

'Against this background it is still necessary to consider the question: if a public authority has information that has been deleted from computer records is it still held? The Tribunal understands that information that is held electronically and then deleted (and even emptied later from a recycle bin or trash can) is in fact still retained in its original form on the computer system until it is subsequently and actually overwritten by other information. In other words, information may be deleted and emptied but it is not actually eliminated from the system at that point. This is the case with most computer systems today, although no two systems will be identical, in terms of their treatment of deleted material. It will thus be a matter of fact and degree, depending on the circumstances of the individual case, whether potentially recoverable information is still held, for the purposes of the Act.'

### Assessing the relevance of electronic documents in a fractured environment

One of the most critical parts of the discovery process is assessing the relevancy of materials. This task is rendered much more difficult in a fractured environment, because the assessment of relevancy is just as much about context as content. If electronic documents are poorly managed the risk of misunderstanding the proper context is significant, which can lead to a substantial risk of failure of discovery. Relevant materials might be improperly withheld and privileged materials might be improperly disclosed.

Again, the problems are magnified where email is concerned. There are many reasons for this. For example, senders of emails might use the blind copy field. Where this context is overlooked the organization could also overlook the existence of potential witnesses. Like a domino-effect, this can lead to a cascade of breaches of the rules. Similarly, senders and recipients of email might print hard copies, the fact of which might not be appreciated; again, the litigant is put at risk of breach of the rules. Furthermore, the body text of email can be easily manipulated after the fact, which might not be apparent in the fractured environment. Finally, emails are connected to computers, not people; in a fractured environment it might not be appreciated that the sender of an email, or indeed the recipient, was the person to whom the email account was assigned.

### Arguing reasonableness in a fractured environment

The CPR contains the caveat for reasonableness for obvious reasons; unlike paper documents electronic ones can soon multiply out of control, they can be subject to many different storage environments and locations and they can be under the control of a much larger number of persons. Consequently, e-discovery can often be an onerous, time-consuming and expensive task, quite out of kilter with the importance of the case and the issues. Thus, the rules contain the caveat that searches for electronic documents must be 'reasonable'.

In a fractured environment e-discovery becomes an even more onerous, time-consuming and expensive task, but it is a fundamental principle of most systems of civil justice that litigants should not be rewarded for their own failures or want of diligence. For this reason the rules place a burden of proof on the party trying to resist discovery.

The inevitable problem for the poorly managed company when addressing the reasonableness of discovery is that they face the very great obstacle that it is their poor systems that are the cause of the problem, not the obligation to give discovery. However, the well-organized opponent will be bound to advance an argument to the court to that effect. It is the writer's experience that this argument very often meets with success; after all why should a poorly managed organization be in a better position to avoid discovery than the well managed one?

E-discovery can often be an onerous, time-consuming and expensive task, quite out of kilter with the importance of the case and the issues.

## AUTHENTICITY IN A FRACTURED ENVIRONMENT

As indicated earlier, electronic documents, particularly emails, are much more vulnerable to amendment, alteration, loss and destruction in a poorly managed environment than in a properly managed environment; indeed, it is the writer's experience that the 'ephemeral' nature of email often attracts arguments about authenticity.

There is no doubt that electronic documents are admissible in evidence; that is why it is subject to the discovery process. However, admissibility is only one component of proof. Evidence needs to be of sufficient probative value, or 'evidential weight', to discharge the burden of proof. If the evidence is not of sufficient probative value the court will discount it, or accord it less weight.

Astute litigants will regularly consider the extent to which the probative value of electronic documents can be challenged. If the electronic documents result from a fractured environment the prospects of a successful challenge are significantly increased; if the provenance of an email cannot be proved to the satisfaction of the court, because it has not been kept in a safe and tamper-proof environment, the outcome of the case might be affected. Thus, attacking the authenticity of email is often a highly productive tactic.



## CASE STUDY

In May 2007 WPP boss Sir Martin Sorrell settled a libel action against two former WPP executives, which arose from the sending of a false image by email. All parties relied upon evidence about the provenance of the email, but due to gaps in the evidence Sir Martin could not prove that the defendants themselves had sent the email. Following the settlement of the case the defendants accused Sir Martin of “fleeing the battlefield”. The failure of the litigation cost WPP approximately £1 million in legal costs.

## CASE STUDY

In a recent case, the writer was defending a group of businessmen who were accused of stealing a company database. The evidence against them was compelling; there were emails passing between some of them, which referred to the possibility of them setting up in direct competition with their employer. Some of them had motive to set up in competition, due to poor quarterly sales and failed business development projects. Importantly, they had opportunity; they had legitimate rights of access to the company database. Finally, there was evidence that the database had been downloaded from a PC that was used by one of the group. Not surprisingly, the company thought that it had a ‘killer’ case.

However, the company were forced to withdraw. Although the ‘visible’ evidence seemed to point only one way, there was a huge amount of ‘invisible’ evidence that fatally undermined the company’s case. This invisible evidence was found in the fact that the company had a fractured environment for data processing and ESI. Whereas computers were password protected, passwords were weak, often shared and never changed. Although there were hard copies of emails available, the electronic versions had been irrevocably deleted and there were no archive copies. Even though the group had motive, so did other company personnel. Where the emails seemed to have passed between the group, they had actually passed between computers.

The failure of the case was 100% attributable to the fractured environment. If the use of email had been properly managed, with proper access control mechanisms and a proper email archive, the company would have won the case, yet they managed to snatch defeat from the jaws of victory.

## LITIGATION THAT IS COMMONLY CONCERNED WITH EMAIL

Litigation, civil and criminal, can arise from the use and misuse of email in many different ways:

- The civil and criminal offences of harassment under the Protection from Harassment Act involve a course of conduct that causes distress. The sending of harassing emails can amount to a course of conduct.
- A libel occurs where a person makes a statement to another about a third party that causes the other to think less of the third party. Obviously, emails can be used to communicate libelous statements.
- The Malicious Communications Act criminalizes the sending of 'hate mail', which includes the sending of hate email.
- A person can breach their duty of confidence in confidential email through the sending of an email to another person.
- Emails can be used to send infringing copies of copyright protected materials.
- Unlawfully obtaining personal data contained in emails is a criminal offence under the Data Protection Act.
- Using a computer without permission to gain access to emails is a hacking offence under the Computer Misuse Act.
- Disclosing emails without permission or lawful authority can infringe a person's right to privacy under the Human Rights Act.
- Intercepting emails without lawful authority is a criminal offence under the Regulation of Investigatory Powers Act.
- Distance contracting by email where the seller neglects to provide core information about themselves and their business is unlawful under the Consumer Protection Distance Selling Regulations.
- The sending of spam emails is unlawful under the Privacy and Electronic Communications (EC Directive) Regulations.

Within a fractured environment the organization carries an unascertained risk of breaching the law in literally thousands of different ways.



## 12 STEPS TO ENSURING GOOD EVIDENTIAL QUALITY OF EMAIL

As a litigation attorney who specializes in email law, I would suggest taking the following steps to maximize the evidential quality of your email. An organization that adopts these 12 steps will be well equipped to cope with an e-discovery exercise, whether that is for the purposes of litigation or for the purposes of a regulatory investigation. These steps will provide the best environment for meeting the tight timetables within the FRCP, they will enable the organization to properly assess the relevance of materials,

they will provide very strong ammunition for arguments about the reasonableness of discovery and they will provide the organization with an almost cast-iron position on the question of authenticity.

And, of course, most important of all, they will equip the organization and the attorney with the position they need to take control of litigation, which will always increase the prospects of success.

- 
- 1. Ensure the use of email is subject to agreed procedures, which are supported and enforced by management at a high level. Acceptable use policies must prescribe good usage and identify bad usage.**
  - 2. Train users of email in acceptable use, and their rights and the obligations expected of them.**
  - 3. Implement access control mechanisms to computer systems – so that use can be attributed to a person, a terminal, a date and a time.**
  - 4. Ensure computer systems are kept safe and secure, so that the systems and the data within are protected from unauthorized access and accidental or deliberate loss and damage.**
  - 5. Retention and deletion of email should be organization defined, not user defined. Individual users should not have any discretion as to the categories of emails that should be retained or deleted.**
  - 6. Implement a solution that archives and stores emails centrally. The archive should support all the main file formats and also retain metadata.**
  - 7. The archive should classify emails entering the archive at the point-of-entry. The archive should prevent the entry of duplicates.**
  - 8. Ensure the archiving platform facilitates the exporting of evidence as files as a part of the e-discovery process.**
  - 9. Implement an archiving solution that allows full search and retrieval. Metadata should be searchable as should content.**
  - 10. Enable logging of all events acting on the archive. The logs should be retained as part of the archive, for auditing and verification purposes.**
  - 11. Provide contingency for continuity of both archiving and discovery in the event of an outage.**
  - 12. Ensure the archiving platform supports the marking-up of files, so that privileged materials can be withheld and/or redacted during e-discovery.**

## SOURCES

1. The Sedona Conference is a US think-tank whose mission is to advance the development of the law. Its 'Sedona Principles' categorize types of electronic documents for litigation purposes. In 2005 the Commercial Court for England and Wales endorsed the Sedona Principles and incorporated their essence within amendments of the CPR, so as to clarify the scope and ambit of e-discovery.

## ABOUT MIMECAST

Mimecast Services for Microsoft® Exchange, Outlook®, Windows Mobile® and Blackberry® provide enterprise-level email continuity, archiving and security for any size of company. 'Unified Email Management' requires no hardware or software, integrates with an organization's existing IT, offers complete control to the IT administrator and takes just hours to set up.

Every day, Mimecast takes care of millions of emails and documents for thousands of companies around the world. Founded in 2002, Mimecast has operations in North America, Europe, South Africa and Offshore.

**North America**

275 Grove Street,  
Building 2, Suite 400,  
Newton,  
MA 02466

tel: 1 800 660 1194

email: [info@mimecast.com](mailto:info@mimecast.com)

**UK & Europe**

2-8 Balfe Street,  
Kings Cross,  
London,  
N1 9EG

tel: +44 (0)207 843 2300

email: [info@mimecast.com](mailto:info@mimecast.com)

**South Africa**

Morningside Close Office Park,  
Block G, 1st Floor 222 Rivonia Road,  
Morningside

tel: 0861 114 063 (S.A. local)

tel: +27 (0)112 585 300 (intl)

email: [info@mimecast.co.za](mailto:info@mimecast.co.za)

**Offshore**

The Powerhouse,  
Queens Road,  
St Helier,

Jersey, JE2 3AP

tel: +44 (0)1534 752300

email: [info@mimecast-offshore.com](mailto:info@mimecast-offshore.com)

[WWW.MIMECAST.COM](http://WWW.MIMECAST.COM)