The myth of email as proof of communication

Increasingly, there is a need for organisations to be able to prove the content of communications between themselves and other parties. Such proof has been difficult to achieve in the past – systems were mainly dependent on each party utilising the same

November 2016

Organisations are facing an increasing need to be able to show exactly what was communicated, to whom and when. The ubiquity of email provides an ideal means of doing this, but it needs additional capabilities; to ensure that the email is stored in an immutable form and is timestamped, in a manner whereby the document can be seen as being legally admissible as evidence.

Whether the need is for ensuring that contract terms are acknowledged and enforced, keeping records of online sales, protecting key information, or whatever compliance requirements or regulation a company must meet, being able to reference an immutable copy of communications between parties has immense business value.

Essentially, if anyone in an organisation has ever said, "Just what did we communicate at the time?" then a means of evidential proof is required.

Clive Longbottom
Quocirca Ltd
Tel : +44 118 948 3360
Email: Clive.Longbottom@Quocirca.com

Rob Bamforth
Quocirca Ltd
Tel: +44 7802 175796
Email: Rob.Bamforth@Quocirca.com

Executive Summary

The myth of email as proof of communication

Proof of what was communicated between parties can help deal with disputes between organisations and their various stakeholders, including customers, suppliers, investors, government and regulatory agencies, as well as providing proof of compliance to trade body or to meet government legal needs.

Proof of communication is an increasing need

Verified, immutable proof of what, to whom and when was communicated can help make life so much easier for all involved. Whether it is to show a loyal customer what was promised; a fraudulent customer that their claim is not valid; a supplier what it was that was really ordered; a trade body the documents that are sent out to people; a government body what communications are entered into with different parties or whatever, such proof can be invaluable.

Despite the headlines, email remains ubiquitous

Although the media point toward a reduction in email usage, email remains the most prevalent technology for person-to-person communication today. The rise of apps such as WhatsApp and Telegram are touted as email replacements – but these are proprietary systems that generally require both sides to be using the same app. Even where individuals have moved over to real-time chat for much of their person-to-person communication, they still use email for communicating in a more formal manner – both in B2B and B2C environments.

Ensuring that email is admissible is the real requirement

Emails can be altered – not only the message content and attachments, but also the date sent, date received, who the message was sent to, from whom: absolutely anything in an email is alterable by someone with enough knowledge. As such, no email has legal admissibility on its own, when the other party is denying its authenticity. Therefore, the key is to create an immutable copy of the email and its metadata that would be admissible – if it ever came to such a need.

Avoidance of court saves time, money and reputation

The idea with legally admissible immutable records is not necessarily to be able to wave them at a judge in court, but to stop any problems at as early a stage as possible. By being able to prove what was communicated, the majority of disputes can be dealt with quickly and effectively to both parties' satisfaction, and at the lowest cost possible.

Immutable documents also cut abuse and fraud

For instance, Fintech companies are bringing simpler, quicker and cheaper ways to be granted credit, in a similar way to that in which online retail has changed how we buy. Allowing quick and convenient access to credit or to products requires a capability to foresee and stop problems that can have a serious impact on business profitability. As well as providing a highly efficient means of dealing with issues when they arise, if a company chooses to make it clear, as part of the message that it has been stored in an evidentiary manner, those attempting a malicious fraud will be put off from trying in the first place.

Reliable email records need specific skills

Setting up an organisation's own means of creating immutable email records is not easy – nor would it be cost-effective. With highly specialised providers on the market who can act as email proxies for messages, creating full records with timestamps for very low costs, it makes far more sense to look to such a provider, than to a 'build your own' approach – plus it provides a greater level of independence to the document's provability.

Conclusions

Email remains ubiquitous, and provides a solid platform for communicating information between parties. However, in itself, email is not a final-form content mechanism – what is required is to register its contents and delivery as an immutable record receipt that can be stored, searched and retrieved as required to meet an organisation's needs. The use of 'assured delivery' of 'immutable content' emails via an external third party provider meets these needs.

Avoiding costly confrontation

An organisation may find that it needs to prove what has been communicated electronically to others. To consider that the saying “I sent it by email!” was enough of an argument has not only been a wrong assumption, but also a myth. This is why the argument needs to come down to, who communicated what, to whom, when and in what way – in many cases ending up in front of some form of mediator or even a court of law.

> *“[The] need to provide evidence of what was communicated and when goes beyond being able to prove to customers or suppliers what was communicated to them (and by them). It can also be used in internal and external governance, being able to show to industry regulators (such as the FCA, ISO groups or vertical market certifying groups) that an organisation is compliant with their needs, or to central government bodies that an organisation is compliant with the needs of the applicable regulations.”*

Any such steps have costs to the organisation. Even if the organisation wins its case, the preparation of what it needs as evidence for building its case will be expensive, and there is always the risk of damage to the organisation’s brand, even after winning, as the press and public could take more of a “David and Goliath” view and be supporting the underdog of the claimant.

The need for an organisation is to avoid such cases going to court – but to do so it has a requirement to show that if the claimant wishes to take the case further, then the amount of evidence that could be provided by the organisation is so overwhelming that taking such steps would be unadvisable.

This need to provide evidence of what was communicated and when goes beyond being able to prove to customers or suppliers what was communicated to them (and by them). It can also be used in internal and external governance, being able to show to industry regulators (such as the Financial Conduct Authority (FCA), ISO groups, or vertical market certifying groups) that an organisation is compliant with their requirements, or to central government bodies that an organisation is compliant with the needs of the applicable regulations.

However, having the capability to create, manage, recover and present this proof of communication has proven difficult in the past. Certified paper-based mail, such as that provided by the UK’s Royal Mail ‘Signed For’ service, is far too costly in most cases. Indeed, one company that changed its trading name had to send notifications to millions of people. It started by using signed for paper mail – but the costs of printing, folding, enveloping, addressing, sending via a bulk mailing company and so on were totally impractical. It did not take long for the company to realise that email was a far more cost, and process, effective approach. One of the problems with paper mail is that proving what the recipient received is not totally possible – it has often been the sender’s word against the recipient’s. The use of delivery and read receipts on emails (known as message deliver notifications (MDNs)) is easy for users to get around, either by setting up email clients to refuse to provide such receipts or through challenging whether the sender has the right email address details. Even where such receipts exist, the same problem as paper mail exists: it cannot be used to prove what was sent as the content itself is not immutable – and so many interactions simply become an argument over whose version of the truth can be trusted.

> *“The use of delivery and read receipts on emails (known as message deliver notifications (MDNs)) is easy for users to get around, either by setting up email clients to refuse to provide such receipts or through challenging whether the sender has the right email address details.”*

This paper looks at how a ubiquitous technology – email – can be easily used to ensure that this body of proof can be created and managed – and how this can lead to a reduction in costs when dealing with dissatisfied customers, an avoidance of fraud and help an organisation demonstrate its compliance to internal and external governance risk and compliance (GRC) needs.

The burden of proof

Over the past few years, in the UK alone there has been a raft of highly reported cases of the mis-selling of goods and services, such as endowment-based mortgages, payment protection insurance (PPI), credit card loss insurance and so on. Each of these areas could have had the interactions between the claimant and the company involved streamlined if proof of communications and the content of those communications could be provided at as early a stage as possible.

Less well reported are cases where a person pays for an item using a credit card, and then claims back against the merchant on the basis that they either never received the goods or that the goods were not as described. The merchant then either capitulates and refunds, or refuses to repay. On refusal, the customer may then refer this to the credit card issuer as a claim.

> *"Over the past few years, in the UK alone there has been a raft of highly reported cases of the mis-selling of goods and services, such as endowment-based mortgages, payment protection insurance (PPI), credit card loss insurance and so on. Each of these areas could have had the interactions between the claimant and the company involved streamlined if proof of communications and the content of those communications could be provided at as early a stage as possible."*

In the case of such claims, the credit card issuer generally refunds the money to the customer and then recoups it from the merchant. This approach, known as 'chargeback', puts the merchant in a bad position – they find it difficult to prove to the credit card company what was presented to the customer, and this lack of evidence counts against them. The merchant is out of pocket – they have had to pay the credit card company back the amount that the customer had paid – and it is difficult for them to recover the goods from the customer. With physical goods, there is, at least, a chance of identifying that the recipient received them (e.g. via courier tracking), but with electronic goods, such as music, videos, travel/event ticketing, etc., it is generally just the word of the customer against the merchant. Such cases are on the rise – and the lower financial limit for chargeback cases to be considered by the credit card company is being matched with higher per-claim administrative charges. Visa estimated fraudulent chargeback to be running at $11.8b in 2012[1]. However, the growth in chargeback cases is reported to be running in double figures (up to 19% in some findings), with retailers suffering from 0.3% to 5% of their credit card-based sales being subject to chargeback claims. Although a proportion of these will be either legitimate or an easily disproved claim, an increasing percentage are from individuals trying to defraud a company. Indeed, some research points to up to 86% of claims being fraudulent – and over 50% of people going straight to the card issuer, rather than to the merchant first. When the average consumer is filing a chargeback as the primary method to get a refund, the system is broken.

> *"The idea with being able to show exactly what a buyer had in terms of communication, and in many cases with electronic goods, what they actually received, should not be viewed as a means of demonstrating in court that the buyer is in the wrong. The idea is to rapidly and extremely cost-effectively demonstrate that the buyer's case is without any merit – and so to get them to rescind any claim and pay what is due."*

The costs of chargeback are not just those 'hard' costs of the loss of money from paying the card company the transaction amount plus the administration fees (which can range from a non-reversible fee of $5 to $35 per chargeback), but also in the time spent by the merchant in dealing with the issue, and in investigating the case to see if it is a valid claim or not. It can also affect the merchant's capability to use certain means of card payments. Many card providers work on the basis that if a certain proportion of transactions become liable to chargeback, then the card provider can prevent the merchant from using their service.

[1] http://www.dailyfinance.com/2014/03/20/friendly-fraud-costs-retailers-billions/

"However, prevention is generally better than a cure. The main idea of having legal proof of an exchange of information should not be so that court cases can be entered into with a better chance of success. Legally provable documentation helps those who are trying to be good – the honest customer and merchant; and makes life harder for those trying to make a maliciously fraudulent claim."

The idea of being able to show exactly what a buyer had in terms of communication, and in many cases with electronic goods, what they actually received, should not be viewed as a means of demonstrating in court that the buyer is in the wrong. The idea is to rapidly and extremely cost-effectively demonstrate that the buyer's case is without any merit – and so to get them to rescind any claim and pay what is due.

This persuading of complainants to settle rapidly before any escalation of the case can then be used to eventually dissuade customers from attempting such claims in the first place; through showing on the merchant's web site and in its documentation how the merchant deals with such cases. As the burden of proof moves from the merchant to the buyer, there is less attraction in a buyer attempting a chargeback claim. In a recent move, both Visa and MasterCard have stated that they will accept certain evidential electronic data as proof that chargeback should not be allowed. Such 'compelling evidence' needs to be just that – an evidential copy of communications meets the requirement.

There are many other areas where the need to prove information was provided is important. For example, a change in the terms and conditions of a subscription or service needs new documents to be sent to the customer, but also requires proof that they were sent – and what was sent on what date.

Likewise, proof of guarantee – either what was stated within the guarantee, or the date from which the guarantee started - can help in ensuring that customers know both exactly what they agreed to at the time of purchase and whether they are still in the period of guarantee, or not.

However, prevention is generally better than a cure. The main idea of having legal proof of an exchange of information should not be so that court cases can be entered into with a better chance of success. Legally provable documentation helps those who are trying to be good – the honest customer and merchant; and makes life harder for those trying to make a maliciously fraudulent claim. Areas of dispute are rapidly dealt with, and if the merchant decides to provide a service (such as a product replacement or refund) that is outside of the provable previously agreed terms and conditions, then it will be seen as a more positive act by the customer. Life is made harder for the casual fraudster – when faced with legal proof of what information they had at their disposal, many will cease their claim at that point.

"The need for proof of communication is widespread – there are many more cases where such a need exists than have been mentioned above. Any organisation that has found itself at any time in the position of asking, "Just what was communicated?" has the need.

The problem is, just how can this be done in a manner that is both workable and cost-effective?"

Other areas where proof of communication can be useful include where an organisation needs to carry out a product recall or issue a product advisory. Being able to show that customers did receive such documents – and what was in those documents – can be important should something happen after the advisory has been issued. Being able to show that the customer was warned about a possible fault, about the risk and complexity of the product and the steps that they should have taken, could well be needed.

There is also a need for proof of information exchanged in business-to-business (B2B) situations as well. The need to prove what was ordered, what changes were requested and what terms and conditions were applied against an order, all requires solid proof of documentation that can be shown to have been sent at a specific time.

The need for proof of communication is widespread – there are many more cases where such a need exists than have been mentioned above. Any organisation that has found itself at any time in the position of asking, "Just what was communicated?" has the need.

The problem is, just how can this be done in a manner that is both workable and cost-effective?

The ubiquity of email

Many things have been tried to provide a means of provable delivery of information. From the days of hand-delivered paper mail, through Telex to electronic data interchange (EDI), some approaches have proven more robust than others.

The problem with the current methods, such as signed-for delivery of hand-delivered mail or the use of EDI or receipted file transfer protocols (FTP) is that they are either slow or expensive to use – in most cases, both. EDI and FTP also require the receiving party to have the equivalent tools in place – and even with B2B information, this cannot always be the case, and with consumers has to be assumed to be the exception rather than the rule.

What has to be used is a method of getting data to anyone in an easy manner. The easiest and most cost-effective manner across the world at the moment is email – a communication that is called a 'durable medium' within the EU Directive on Consumer Rights and in the UK Consumer Rights Act.

> *"Although Quocirca sees the headlines of 'email is dead' every time a new mode of communication comes to market, email is still very much alive. There has been a rise in the use of technologies such as Skype, WhatsApp and Telegram, but these are proprietary technologies tied in to only being able to interact with others using the same technology. The same goes for the recent announcement of Facebook at Work – currently touted as the latest email killer; it is just another approach that is still constrained by the need for all parties to be using the same proprietary technology."*

Although Quocirca sees the headlines of 'email is dead' every time a new mode of communication comes to market, email is still very much alive. There has been a rise in the use of technologies such as Skype, WhatsApp and Telegram, but these are proprietary technologies tied in to only being able to interact with others using the same technology. The same goes for the recent announcement of Facebook at Work – currently touted as the latest email killer; it is just another approach that is still constrained by the need for all parties to be using the same proprietary technology. Email is fully standardised – it makes no difference what email client application either the sender or recipient is using. An email sent from anyone in the world to another person anywhere in the world will be received and, providing both parties speak the same language, will be fully understandable. Indeed, the Radicati group states that 109 billion business emails were sent in 2014, with an expected volume of 139 billion emails per annum by 2018. Radicati also predicts that email account numbers will grow from 4.1 billion to 5.2 billion over the same time, with the current 2.5 billion individual users growing to over 2.8b[2] – or around one third of the total population of the planet.

Therefore, it is likely that when dealing with another entity (consumer or business), there will be an email address that can be used to send the data to.

This ubiquity does not make an email a legal document, however. It is easy for an email to be tampered with, have its timing changed, who it was sent to or by, its actual content and so many other areas. Therefore, just having the capability to show an email at any time can soon become a case of one person's (or group's) word against another. While it may be enough to persuade some people to call off a complaint against the company, for many, who

[2] Radicati Group, April 2014, http://www.radicati.com/wp/wp-content/uploads/2014/01/Email-Statistics-Report-2014-2018-Executive-Summary.pdf

understand how email works, they know that it is simple to claim that what one person sent as an email is not what they received.

Historically, organisations have attempted to use simple approaches such as delivery and read receipts to show that an email reached its destination. The problem here is that a lot of people now turn off these notifications, and they cannot be relied on to prove or disprove anything. Indeed, delivery and read receipts were never meant to be a legal form of proof. Known as a message disposition notification (MDN), the IEEE, under which the standards for email falls, states in RFC3798 that '*MDNs may be forged as easily as ordinary Internet electronic mail (…) do not provide non-repudiation with proof of delivery'* and *'cannot be relied upon as a guarantee that a message was or was not seen by the recipient'*[3].

Others have tried inserting a live button or link within the message, requesting people to click on the button or link to agree that they have received the message. Again, though, all it needs is for the recipient to choose not to do so (or neglect to do so) and any provable evidence of information sent is then unavailable. Even where such a receipt is gained, it still suffers from the same issues – it could have been manually created or its content could have been changed.

Another approach is to embed a 'hidden image' into the message. This image is identified via a URL, the idea being that the opening of the message will trigger that URL and so notify the originating server that this has been done. However, as this approach has also been used by hackers to download malware onto people's machines, most organisations and most email client software now prevent the automatic downloading of remote images. Such use has its role in campaign tracking; it has no role to play in evidential content management.

Therefore, a system is required where there is little to no setup at the sending end and requires no setup or actions to be taken whatsoever at the receiving end, nor necessarily informing the recipient about it. This is where systems that work against 'assured delivery' come into play.

The law and information

> *"A full record of every communication between the organisation and the customer could have been used in some cases to show that the person had agreed to certain material points and that they were fully apprised of possible issues and of the risk and complexity of products before they agreed to the deal."*

The exchange of information between parties is governed by many different laws. From the need to ensure that any personally identifiable information (PII) is dealt with securely, in any legal/business context, it is important that any organisation ensures that it and any partners in the information delivery process are operating within the law.

Bear in mind that, if the message being sent breaks any of the information laws, a legally admissible copy of that document will be proof that the sending organisation has broken that law. Therefore, it is important to have the right tools in place to validate messages before they are sent, using approaches such as data leak prevention (DLP) and information redaction (the physical blanking out of certain data as required, such as National Insurance numbers or full credit card numbers).

Banks and other financial services companies in the UK also have to work to rules imposed by the Financial Conduct Authority (FCA), which replaced the Financial Services Authority (FSA) in April 2013. As the body that has authority over how financial services are marketed, it is important that organisations falling under its remit can prove what communications were entered into between themselves and a customer. In many cases, this may need to be done years after the initial deal was struck – issues around pensions, endowments, payment protection insurance (PPI) and so on only came to a head many years on. A full record of every communication between the organisation and the customer could have been used in some cases to show that the person had agreed to certain material points and they were fully appraised of possible issues and of the risk and complexity of products before they agreed to the deal.

[3] https://tools.ietf.org/pdf/rfc3798.pdf

Case study

Primal Game Studio

Primal Game Studio is a video game developer based in Budapest, Hungary.

Business problem
Primal deals with a lot of electronic assets – video files, code, contracts and so on that are vital to its business. Primal recognised that whereas physical assets had a model around them for providing proof of delivery via physical receipts, it was harder to do so for electronic items.

Thought process
Primal wanted a solution for electronic assets that replicated those it saw in the physical world. Months of research proved fruitless, until Primal approached eEvidence to discuss a possible solution.

Solution chosen
Primal chose eEvidence's solution as it met its needs exactly. Not only did Primal gain evidentiary proof of the delivery and content of emails, it also knew that these were compatible with EU regulations.

Business benefits
Primal now has confidence in that its intellectual property is secured when sent by email to any recipient worldwide.

For those financial services companies that are within the scope of the markets in the financial instruments directive (MiFID), the need to capture, track and prove communications between parties is of paramount importance. The use of the MiFID 'passport' (as first dictated under the previous investment services directive (ISD)) now enables such financial services companies to operate across the whole of the EU. Being able to demonstrate exactly what was communicated, between whom and when helps to meet the client-order handling, pre, and post-trade transparency needs of the MiFID framework, whilst also ensuring that all parties have access to immutable proof of such communications.

For those who have a problem with a financial institution, they can go to the Financial Ombudsman. The Ombudsman has statutory powers behind it, via the Financial Services and Markets Act 2000, but cannot make binding decisions. Those unhappy with the Ombudsman's findings can still take the matter to a higher court. However, for a financial services company, there are case fees to pay should a case go to the Ombudsman – and again, by being able to demonstrate to a complainant that their case has little merit, such expense can be avoided.

The UK has many similar bodies – for example, in the telecommunications sector, Otelo and CISAS are the ombudsmen that consumers can use to try and gain a resolution in a complaint about their telecommunications or internet service provider. Ofgen acts on issues around energy suppliers. ABTA and AITO act on matter concerning travel. There are many trade bodies to act for different trades – such as TGO and DGCOS in the glazing industry, and so on. In many cases, there will be more than one trade body ombudsman – but being able to provide full provable details in any case can help to avoid the need for a case to go through the process in the first place.

With credit card chargeback, some areas will fall under legal directives, such as the EU Directive 2008/48/EC and the UK Consumer Credit Act 1974/2006. However, the main area of worry for those involved in transactions where a card and cardholder are not present is the 'friendly fraud' – currently estimated by Visa to be costing over $11b per year. Here, a buyer purchases a product, generally online, and then raises a chargeback claim via the credit card issuer (i.e. the cardholder bank). The credit card issuer provides a refund, and it is then down to the e-merchant to prove that a product has been delivered or used. Although a percentage of friendly fraud is accidental (an individual seeing a transaction on their bill and not recognising it, so requests a chargeback), the majority is maliciously fraudulent. It is also aimed at goods that are of a lower value, making it cost-ineffective for retailers to jump through all the hoops required by the credit card companies to prove the sale did happen and the goods were delivered.

By putting in place evidential proof of communication, it is easy to head off such fraudulent activity. As soon as a claim is lodged, the e-merchant can show exactly what was sent as email communication. For the accidental claim, this will be enough to remind the purchaser what they received. For the malicious fraud, it provides enough evidence to challenge the chargeback – and, if necessary, can be used as a deterrent by marking communications as an evidentiary document when originally sent to the buyer.

A further area of legality around email and electronic documents is the use of physical signatures. The Electronic Communications Act 2000 defines what is acceptable as a means of identifying a document as a 'signed' document. A physical signature on a paper document is still the main means that people tend to regard a document as having been signed. With the advent of more digitised workflows, the Act accepts that a scanned physical signature, an electronically created signature or an eSignature created by a validated body, are acceptable to show that a document was signed. However, such signatures are just part of a message's content – the document itself can still be altered through electronic means without it affecting the signature – so it yet again becomes a case of one person's word against another. Although signatures are often a perceived requirement, ensuring that the content is evidentiary is still necessary – these approaches should be seen as being complementary, rather than an either/or decision.

The Act also allows for an electronic action taken by a party – such as clicking on an 'Accept' button – to be seen as legal acknowledgement. However, such actions do not provide a solution that can be deemed to be content of a 'durable medium'.

The Court of Justice of the European Union (EJC) determined that links back to a retailer's site did not meet the needs to be seen as a 'durable medium', nor those of the Distance Selling Directive. Therefore, the use of an 'Accept' button may not be enough, unless the terms and conditions are presented and delivered to the recipient in a saveable form prior to any commercial action being entered into and that these Ts&Cs are then irrevocably linked with that electronic action. An eSignature still does not guarantee the content of the document has not been altered, unless the document has been sent under the auspices of a digital/information rights management (D/IRM) system. Such use of D/IRM is outside the scope of the majority of organisations. Therefore, using immutable content email approaches alongside eSignatures is still recommended.

The law and admissible evidence

Only a few countries have created laws around what constitutes legally admissible electronic documents. This is due to the perception that information in electronic form can be altered in many ways, and that proving that any content is 'original' is problematic.

However, there is broad agreement across the EU and the US as to what would be acceptable as an evidential electronic document. Based on a definition by Eoghan Casey in 2004 in his book "Digital Evidence and Computer Crime"[4], admissible electronic evidence is as such:

> "Digital evidence or electronic evidence is any probative information stored or transmitted in digital form that a party to a court case may use at trial. Before accepting digital evidence, a court will determine if the evidence is relevant, whether it is authentic, if it is hearsay and whether a copy is acceptable or the original is required."
>
> Casey, Eoghan; Digital Evidence and Computer Crime, 2004

[4] https://www.elsevier.com/books/digital-evidence-and-computer-crime/casey/978-0-12-374268-1

Use case scenario

A global top-10 fintech company

This fintech company, deemed to be in the global top ten by KPMG and H2 Ventures, needed a means of legally notifying its customers when it had terminated a credit agreement with them when the customer had missed payments. The notification would also confirm that debt collection processes had been initiated.

The company required that the notification be delivered as a 'durable medium'. Although the company believed that a standard email met the requirements in most of its markets, it was assured that such a delivery mechanism would not meet the legal requirements in Poland.

The company spoke with eEvidence and based on how eEvidence could demonstrate that its eEvids counted as 'durable media' under EU law, the company enacted eEvidence's system within two weeks across all its markets.

Therefore, any electronic information that is stored with any thought of being used in evidential form needs to meet these requirements.

Ensuring that all communications between parties (i.e. buyers, merchants, service providers) are captured guarantees that the information is relevant. Capturing it in a final, unalterable form along with a timestamp ensures that it is authentic and original. Once the document has been converted into such a final form and timestamped, it can be stored anywhere – it is unalterable without leaving easily visible signs that it has been altered. Organisations can choose to store the documents themselves – or to allow a third party to store them for them, so that they would still be available should some disaster strike the organisation's own storage systems.

This leaves hearsay, which is far more down to the actual content of the documents themselves. As long as the content itself is also relevant, it is likely that a court will allow such information to be entered as admissible evidence.

Such a simple approach to whether content is authentic and admissible at a global level is far better than trying to ensure that all applicable local and regional laws are applied to. As long as the areas mentioned above are covered, it is pretty much assured that the content would be admissible in any court of law.

Assured delivery

What organisations are looking for is a system that does not get in the way of how they do work, nor force their customers to have to have specialised software at their end. Therefore, any chosen system has to be able to work with all known email systems (as it has to interoperate with all possible email systems used by end users and businesses) and that it is independent of the sending system as well.

The only way that this can work is to use a 'proxy' – an external system that works with an organisation's existing email software and ensures that any email that adheres to simple mail transport protocol (SMTP) standards can be effectively logged and delivered to the recipient.

By carrying out this logging, as long as the proxy operator is accepted as a trusted provider by legal bodies, a point of reference is created that can then be used to show that an action, or group of actions, took place around a known period in time.

However, this leaves two main questions – how to set up and use such a proxy, and what should the proxy offer as its service?

The easiest way to use a proxy is to set up a redirect from the company's email outbox to the proxy. That way, senders still address the email in the usual manner with To:, cc: and bcc: fields as required, along with whatever content they need to put into the email body. The message is sent to the proxy, which then takes its actions on the message and forwards it on to the recipient(s), who will receive the email in the normal way.

So, what actions should the proxy take on the emails?

The obvious ones are that it should take the To:, cc: and bcc: recipients and log them against a timestamp – this provides the barest minimum details for future use to show that something was sent to these recipients within a certain period of time.

This still does not take things far enough, though. Although that timestamped information shows that something was sent, it does not show what was sent. Therefore, it is important to also take an unalterable snapshot of the whole message and store this in a way that is independent of both sender and receiver.

In this way, should the receiver attempt to change anything in the message that they have received, or the sender try to claim that what was sent was different to what the receiver received, there is a single point of reference which is irrefutable proof of exactly what information was exchanged.

Therefore, the basis of what an email assured delivery proxy must provide can be taken as:

- **Simple setup** – No software installation required at the sender's or receiver's end. Emails from the organisation are sent via an email proxy through the provider's system, where the message is securely finalised and either stored or sent back to the organisation, as well as being sent on to the recipient – with the option of this being carried out without informing the recipient.
- **Massive scalability** – Whether an organisation is sending single emails or mass emails, it wants to be assured that the proxy can deal with the message volumes needed. Make sure that the proxy supplier has the capabilities to deal with this – ask about the platform they use and if they have any upper limits in how many emails they can deal with.
- **Final form snapshot** – The capture of the whole message as an immutable PDF document, which is then either stored within the proxy's own environment or sent back to the organisation for storing in its own systems. The message – this is including eventual attachments – has to be stored as a data set in an immutable format - just storing the text is not legally admissible as it can be altered at any time.
- **The right metadata** – Ensure that the right metadata is also stored along with the message. The use of timestamping to show when a message was sent, along with the address the message came from and the address the message was sent to should be the bare minimum. Note that it is unlikely that any case will ever need a timestamp down to the exact hour, minute and second that a message was sent – in the vast majority of cases, the day a message was sent will be enough.
- **Fully auditable** – Is metadata stored to show every step of the process? Can this metadata be analysed and reported against to show the information process and the storage process across the information's life? Such reporting is needed not just for an individual case, but also for internal reporting to show trends in claims and how the system is being used to mitigate losses or how it is being used in other ways.
- **Longevity** – It is impossible to guarantee that an organisation will still be around in the future. It is therefore useless to go for a system that is highly proprietary or that requires the presence of the service company when the evidence of content is required. Therefore, look for a service provider that enables an organisation to store the records on its own site, and that enables the records to be independently verified, for example via the use of hash validation.
- **Use of records, not just items** – In many cases, it will be necessary to pull back many different items to create a complete record of what communications went on between the sender and receiver. Therefore, the proxy

Use case scenario

An online travel company

This travel company required a means of reducing 'friendly fraud' credit card chargebacks.

The company spoke with eEvidence and chose the use of its service to obtain evidential records of all booking confirmation emails sent to customers. Started in mid-2015, the project has already created evidence for over 3 million confirmation emails, ready to be supplied to card companies whenever a chargeback is issued.

The customer has foreseen that the implementation of the service will have a minimum 10% ROI from won chargeback disputes.

should be able to ensure that there is an easy means of finding groups and collections of documents that can be retrieved as a single record.

- **Ease of access** – The sender should be able to access the records at any time and in a short time period. The faster the sender can respond to a customer, the better for all concerned. Such access should not be just via a web portal – the use of application program interfaces (APIs) and JavaScript Object Notation (JSON) document standards means that an organisation can access the information as a web service directly from within its own applications.
- **Secure storage** – If the proxy is storing the records on behalf of the organisation, every record stored by the proxy must be securely stored. Each record contains personally identifiable information (PII), which is regulated under local, regional and global laws.
- **Two-way capability** – As well as being able to use a simple redirect for messages being sent by an organisation to customers, it may be important to also create legally admissible copies of what the customer sends back. If this is needed, ensure that the proxy has the capability to have certain email addresses assigned through to it – whether this be through a simple automatic copy of incoming emails from the organisation's email system, or through the use of specific sub-domain email addresses that go direct to the proxy. For example, all emails from the outside to any email addresses ending in '@response.company.com' could be directed directly through to the proxy.
- **Expertise on how email communications must be dealt with** – Receiving and delivering email is often trivial, but there are many use cases that can be anticipated and must be professionally addressed (i.e. email delivery good practices, delivery errors, sender authentication).
- **Affordable** – If the cost of operating a system is based on a volumetric metric, there is an attraction for a financial person within the organisation to encourage the system not to be used. For example, if it costs, say 50 Euros per person per month, it is financially attractive to only register a few people to such a system. Look for providers who offer a flexible approach – is 'per message delivered' an effective measure for the organisation? Would a tiered approach be better, or a fixed monthly payment no matter how many messages are involved? Providers with a one-size-fits-all pricing policy may be too inflexible to meet a particular organisation's needs.
- **Global** – With the laws around specific content being different around the globe, it is nigh on impossible to ensure that any chosen system will meet each specific legal requirement on a global basis. However, by choosing a system that applies a common sense and self-explanatory approach to creating an immutable document, it is likely such a document will be accepted by any individual or body immaterial of country. Look for a system that makes sense to the organisation; one that uses a standardised and easy to understand approach to proving what content was sent and when.

Conclusions

The power of being able to present to a person, regulatory board or other body exactly what was communicated between parties, and when, should not be underestimated. From simple things such as what terms and conditions were agreed, a notification of an outstanding debt, a communication covering a fault in a purchased item and the steps needing to be taken by the purchaser, through to being able to face down fraudulent attempts to recover money, being able to demonstrate exactly what communications took place between two parties is something that can help cut the costs of arguments between those parties.

Rather than looking at assured delivery of immutable content as a solution to a single problem, it is better that an organisation considers it as an engine that provides solutions for many different issues – ones that are present now, as well as ones that may appear in the future

Email remains ubiquitous – it is a standardised means of exchanging information that is still growing in unique users and volumes of email sent. Other communications methods, whether of a low, or high-tech nature, are not as ubiquitous, are based on proprietary technologies or are far too costly to implement in a broad manner.

Using a cost-effective product where email communications are captured, stored as immutable final form documents and timestamped, with or without requiring the recipient to know or intervene, provides a reliable manner of dealing with the need to prove communication content.

Quocirca recommends using an external third party as a service provider for dealing with emails in this manner. The extra independence of using a third party means that there is even less scope for misunderstanding between the parties involved, and that dealing with any issues based on the communications between the two parties can be more easily and effectively accomplished.

About eEvidence

THE CHALLENGE

Q. Would it be possible to devise a method to supply unquestionable evidence of the contents and delivery of an email, without calling the recipient for action?

A: You bet!

At eEvidence, we believe email can be trusted. It just has to be handled responsibly.

Since 2011, we have worked to make this true. We have created a method that by itself supplies unquestionable evidence of the content and delivery of an email message, without requiring the recipient to intervene – or even know anything about the method itself.

In 2012, eEvidence filed for patents in the US and the EU to cover this method – one that is easy to set up, highly cost-effective and can be used with any email message between any sender and recipient.

For organisations that have ever had to ask themselves “Just what was communicated?” the use of an eEvidence eEvid record can show in a conclusive, evidentiary manner exactly what was sent to a specific recipient on a specific time.

eEvidence in Numbers

Over 10,500 users

Over 60 countries

Over 13,000,000 messages handled

With a successful freemium model, users can start by testing out the method, and can then move to one of our simple and highly cost-effective flat-rate pricing models as required. For massive projects, a fully featured test for processing up to 100,000 emails is at hand and since discounts are built into a tiered structure, the per-email pricing automatically decreases as you send more email.

With customers in the travel, fintech, insurance, pharma, retail and other verticals, using eEvids for governance, risk and compliance (GRC), intellectual property management and in fighting fraud alongside other uses, eEvids are already showing high levels of return on investment for our customers. In fact, eEvidence has over 10,500 users in over 60 countries that have used the method for registering over 13,000,000 messages so far.

More details can be found at http://www.eevid.com

Contact: Carlos Tico
eEvidence
Av. Diagonal, 434
Barcelona
Spain

Tel: (+34) 93 518 1501
Email: info@eevid.com

eEvidence

Follow eEvidence on Twitter at @eEvid

About Quocirca

REPORT NOTE:
This report has been written independently by Quocirca Ltd to provide an overview of the issues facing organisations seeking to maximise the effectiveness of today’s dynamic workforce.

The report draws on Quocirca’s extensive knowledge of the technology and business arenas, and provides advice on the approach that organisations should take to create a more effective and efficient environment for future growth.

Quocirca is a primary research and analysis company specialising in the business impact of information technology and communications (ITC). With worldwide, native language reach, Quocirca provides in-depth insights into the views of buyers and influencers in large, mid-sized and small organisations. Its analyst team is made up of real-world practitioners with first-hand experience of ITC delivery who continuously research and track the industry and its real usage in the markets.

Through researching perceptions, Quocirca uncovers the real hurdles to technology adoption – the personal and political aspects of an organisation’s environment and the pressures of the need for demonstrable business value in any implementation. This capability to uncover and report back on the end-user perceptions in the market enables Quocirca to provide advice on the realities of technology adoption, not the promises.

Quocirca research is always pragmatic, business orientated and conducted in the context of the bigger picture. ITC has the ability to transform businesses and the processes that drive them, but often fails to do so. Quocirca’s mission is to help organisations improve their success rate in process enablement through better levels of understanding and the adoption of the correct technologies at the correct time.

Quocirca has a pro-active primary research programme, regularly surveying users, purchasers and resellers of ITC products and services on emerging, evolving and maturing technologies. Over time, Quocirca has built a picture of long term investment trends, providing invaluable information for the whole of the ITC community.

Quocirca works with global and local providers of ITC products and services to help them deliver on the promise that ITC holds for business. Quocirca’s clients include Oracle, IBM, CA, O2, T-Mobile, HP, Xerox, Ricoh and Symantec, along with other large and medium sized vendors, service providers and more specialist firms.

Details of Quocirca’s work and the services it offers can be found at http://www.quocirca.com

Disclaimer:
This report has been written independently by Quocirca Ltd. During the preparation of this report, Quocirca may have used a number of sources for the information and views provided. Although Quocirca has attempted wherever possible to validate the information received from each vendor, Quocirca cannot be held responsible for any errors in information received in this manner.

Although Quocirca has taken what steps it can to ensure that the information provided in this report is true and reflects real market conditions, Quocirca cannot take any responsibility for the ultimate reliability of the details presented. Therefore, Quocirca expressly disclaims all warranties and claims as to the validity of the data presented here, including any and all consequential losses incurred by any organisation or individual taking any action based on such data and advice.

All brand and product names are recognised and acknowledged as trademarks or service marks of their respective holders.

quocirca