CONVERTING LEGAL & CONTRACT NOTICES FROM PAPER TO ELECTRONIC DELIVERY

A Corporate Counsel Guide

Authored by
Stanley M. Gibson
Partner, Jeffer Mangels Butler & Mitchell LLP

JMBM | Jeffer Mangels Butler & Mitchell LLP

IACCM

Abstract

This white paper was developed in response to a poll conducted by the International Association for Contract and Commercial Management (IACCM) that revealed a growing trend among its members to convert legal notices that are required to be sent by contract (usually by certified mail) to electronic methods. The primary concern among IACCM members was to find an electronic service that would satisfy the requirement to prove compliance, i.e., legally valid proof of what the notice said, whether or not it was delivered, and if it delivered, precisely when.

About the Author

Stanley M. Gibson is an experienced trial lawyer and Partner at Jeffer Mangels Butler & Mitchell LLP, who has focused on high-stakes cases involving complicated technology and bet-the-company cases. For more information, contact Stan at 310.201.3548 or SGibson@jmbm.com.

JMBM Jeffer Mangels Butler & Mitchell LLP

Foreword by Tim Cummins

Today's fast-moving, global business environment demands secure electronic data management and signature systems. These increase speed, safeguard communications and protect against legal or regulatory failures. Yet adoption has been slow, mostly due to a lack of understanding of their possible impact and a lack of confidence in the integrity and security of available systems.

This paper marks a significant contribution to the debate, by providing a robust assessment of the legal concerns and a powerful advocacy of the benefits that can be achieved. It also offers useful parameters that an organization should consider in its selection of an appropriate solution and a perspective on several of the leading offerings.

Tim Cummins
CEO, International Association for Contract & Commercial Management

IACCM

Whitepaper Contents

BACKGROUND:
UNDERSTANDING PURCHASE DRIVERS

A poll of IACCM members representing more than 75 member companies provided insight into the trends in moving legal notices to electronic delivery. In this poll:

- More than half (58%) of respondents report that they intend to convert legal notices to electronic delivery within the next 15 months.
- Most (71%) have hesitated moving legal notices to electronic delivery as they report that they have been in disputes where the recipient has denied receipt of a business critical email. Further, the overwhelming majority (80%) report that they are most concerned with retaining proof of compliance with notice requirements, over time or cost savings (15% and 4% respectively).
- Most continue to send legal notices by paper (receipt mail or courier services); with fax, First Class mail, and standard email being used in approximately equal or lesser amounts.
- For those who have converted to standard email services for sending legal notices, half report having been in a situation where the recipient has denied receipt of an important notice.

Considering these findings, the most important criteria for selecting an electronic service appears to be the service's capability of providing the sender legally valid evidence that he or she has complied with a contract's notice requirements. Noting that IACCM members valued this over time and cost savings with a considerable margin, we believe that IACCM members and other companies will not (and should not) move to electronic notice unless they are satisfied with this requirement. Therefore, we focused on, as primary evaluation criteria, **how well a variety of services would protect the sender against claims of non-compliance with contract notice provisions.**

As secondary criteria, we also looked at administrative time and cost savings.

When evaluating the potential of claims of non-compliance with contract notice provisions, we considered three points:

1. **a claim of non-receipt of the notice entirely**, (i.e. where the electronic message is sent from sender to recipient but the recipient denies having received it),
2. **time of receipt is challenged**, (i.e. where sender and recipient claim time of receipt is different, and the notice is time-dependant), and
3. **electronic message content is challenged** (i.e. sender and receiver dispute the validity or inclusion of certain content including attachment content).

This is a challenging area as it involves the intersection of technology and the law. As such, we prepared the following guidance using simple frameworks that we developed to ease comparison of technology and provide concise descriptions of key legal principles.

SUMMARY OF KEY LEGAL PRINCIPLES

We believe a solution that meets the following seven legal principles would likely yield a legally valid and court admissible piece of evidence to satisfy notice provisions in contracts, should the recipient challenge that proper notice had been provided. These legal principles are summarized as follows:

1. **DELIVERY PROOF:** Provide a record of sending and receiving in accordance with the Uniform Electronic Transactions Act (UETA) by recording the recipient's server's receipt;

2. **CONTENT PROOF:** Use cryptographic techniques to mathematically associate and preserve as tamper-detectable the contents of email and their attachments so as to satisfy process requirements designed under UETA, the Electronic Signatures in Global and National Commerce Act (ESIGN), and in evidence law to establish evidence of content;

3. **OFFICIAL TIME STAMP:** Link to a trusted and objective time source providing essential and credible evidence in disputes in which the time an email was sent or received is material to the case;

4. **ADMISSIBLE EVIDENCE:** Retain records that are court-admissible as to their fact of delivery, as to their legal time of delivery and as to authenticity of content;

5. **FUNCTIONAL EQUIVALENCE:** Serve, under UETA and ESIGN, as the functional equivalent of paper mail, to be used in lieu of certified mail, registered mail, return receipt mail, private express mail services and similar types of paper mail services;

6. **ELECTRONIC ORIGINAL:** Provide a true electronic original of the message content, message attachments, and transmission meta-data including the delivery audit trail; and

7. **CONSENT:** Record consent, as under electronic law the recipient of the electronic transmission must have consented to the use of electronic format as opposed to paper; with a record of the recipient's consent retained as a reproducible legal record to prove consent if challenged.

Importantly, what constitutes a '*legally received electronic message*' is defined within UETA. Assuming UETA applies to the transaction (note, although we are referencing United States law, this principle generally holds internationally as this is based upon a United Nations model law that has been used as the foundation for most electronic transaction laws worldwide), an email is deemed "received" under UETA pursuant to Sections 15(b) and (e), which state the following:

15 (b) Unless otherwise agreed between a sender and the recipient, an electronic record is received when: (1) it enters an information processing system that the recipient has designated or uses for the purpose of receiving

electronic records or information of the type sent and from which the recipient is able to retrieve the electronic record; and (2) it is in a form capable of being processed by that system.

15 (e) An electronic record is received under subsection (b) even if no individual is aware of its receipt.

Similar to when mail is sent, the recipient is deemed to have "received" the email, regardless of whether the recipient is aware of its receipt or retrieves the email, when it enters the recipient's "information processing system" or server, provided that the recipient has designated that system for use, uses it and can access the system.

Note, we recommend that readers review and update all contract notice provisions to include notice by email, if receipt of the email can be confirmed. Some may wish to be more precise and re-state the definitions noted in section 15 of UETA above, to pre-empt any potential issues related to definitions of time of delivery.

We recommend a notice provision such as the one below or one that contains similar language:

"…notice by email if receipt of the email content can be confirmed, with time of receipt being the uniform time the email enters the information processing system that the recipient has designated or uses for the purpose of receiving email."

TOP LEVEL EVALUATION CRITERIA

Protection from Claims of Non-Compliance with Contract Notice Provisions

Description of the Technologies: We will discuss each of the following technologies in the context of what is likely to provide the highest evidentiary weight for proof of compliance with contract notice provisions – legal delivery, uniform time of receipt and content associated with the transaction, and records preserved in a manner that can be authenticated.

A. **Email:** In this review, we considered standard email, as well as email combined with one or more of the following: archive, open tracking (i.e., providing information when a recipient opens the email), time stamps, delivery receipts, digital signatures, encryption, and content verification.

B. **Store-and-Forward File Transfer:** In this review, we considered standard and secure file transfer services with and without open tracking and/or delivery receipts.

   Fax: In this review, we considered standard fax with and without fax logs, and electronic fax with logs and content archive.

Common Misconceptions and Challenges with Standard Use of Electronic Technologies

A. Standard Email: There are challenges when using standard email as a method of delivering legal notices. A summary of the most important misconceptions are:

i. **Printed email:** A printed e-mail (from ones sent folder, inbox, or archive) can easily be denied admission into evidence by simply challenging content authenticity, time of sending, or whether the email was delivered at all; as with a few mouse clicks, one can easily change anything in an email – or the other party can easily claim the sending party altered the email.

ii. **Email copy:** A copy of an email sent to yourself or another person has no bearing as to whether a copy was also delivered to your intended recipient. Email systems are often configured such that internal copies never even reach the Internet and are simply moved from one file directory to another on the sender's email server.

iii. **Electronic archive:** Electronically stored copies of email in an archive of the sender or recipient only provide a record of what the archiving party 'claims' to have happened. Even if the archiving party can forensically prove the content in their archive is authentic, they will be unable to prove delivery or timing of receipt should the recipient claim not to have received it; or authenticity of the sender should the receiver claim to have received a certain email (note, it is very easy, for example, for any receiver to create a false email from any sender and send it into an archive at a specified point in time).

iv. **Bounce notices:** Reliance on bounce notices provide a false sense of security -- most recipient servers turn off bounce notices due to "Directory Harvest Attacks" and "Backscatter Blacklisting" concerns. Therefore, if the sender does NOT receive a bounce notice, they certainly cannot rely on that to demonstrate successful delivery.

v. **Denial of email reception:** IT departments often overlook the complexity of "packaging" ones evidence for presentation to other parties. Importantly, if there is a dispute, how does one present the information to the arbitrator, mediator, judge or jury? How does one show what has been produced is the authentic information – authentic internet records associated with precise content and uniform times of sending and receiving? Litigators can simply point to public research and claim their clients never received the email or request the sender to authenticate that the email was in fact received, what the received content said, and when it was received. For example, Ferris Research, a leading messaging analyst, reports, "3% of non-bulk, business-to-business Internet email goes undelivered to its intended recipient." How do you prove that your critical email notification was not within than 3%?

B. **Store-and-Forward File Transfer:** Store-and-forward file transfer systems are systems that require the sender to upload or send a file (a notice letter in this case) to a central party or server, which stores that file and sends an email to the recipients asking them to visit a website to download the file. This is analogous to sending a postcard to the recipient asking them to visit the post office to pick up the letter. There are two challenges with using store-and-forward file transfer services as a method of delivering legal notices:

i. **Phishing, spamming and security concerns:** People generally do not go through the process of retrieving the information. With store-and-forward systems, most recipients, due to security concerns, being offline, or email overload, do not click-through to collect email. If the recipient does not take action to retrieve and download that file, then the file has not entered their system and notice has not been accomplished – an email is only deemed received under UETA when the recipient's server associated with the designated email address receives the email from the sender.

ii. **Inability to prove notice reception:** Since a standard email is generally transmitted from the store-and-forward system to the recipient requesting the recipient to download the information, the sender has further challenges determining whether or not the recipient has even received the notice to 'collect' the message (see prior section referencing challenges with standard email notification).

C. **Fax:** Most are familiar with the administrative hassles of sending faxes. For the purposes of this analysis, what a standard fax machine does is present a log of 'transmission complete' (assuming a completed transmission) with a notation as to the time and number of pages. The challenges here are as follows:

i. **False Confidence:** Often pages do not get transmitted, or properly transmitted, so a reported successful transmission by the fax device does not mean that the recipient received all of the information or the information in a legible manner.

ii. **Recipient Requirements:** Requires reliance on recipient having a fax machine that is in proper function to receive.

iii. **Ease of Manipulation:** Times on the log or stamped on the fax can be easily manipulated by the sender or receiver.

iv. **Easy to Challenge:** A stapled transmission log attached to the original sent item can be easily challenged for the reasons noted above.

v. **Administrative Issues:** Sending a fax with multiple pages or to multiple recipients gets challenging in terms of ensuring proper transmission and complete page transfers to all parties.

COMPANIES THAT PROVIDE ELECTRONIC NOTICE SERVICE

For this analysis, we focused on solution providers that own the technology that they provide rather than mere resellers or distributors of third-party technologies. Assuming companies would prefer to implement technologies that have proven to be sustainable in the marketplace; we further focused this analysis on providers who have been (a) servicing commercial enterprise customers for more than 5 years, (b) have published testimonials on their website from recognizable companies, and (c) demonstrate the capital resources to continue to innovate. We are assuming that companies that at least meet these criteria are stable and can support the needs of a global deployment.

We did not analyze newer service providers in this white paper due to a risk of inexperience in servicing enterprise customers and sustainability in the marketplace as there is an obvious concern that newer providers may not be around in the long run to service their customers or may be using unlicensed technology patented by others. This could be particularly important if a company needs to go back to the provider for assistance in proving that the electronic notice was actually delivered in a legally compliant manner.

If one is considering purchase from a reseller rather than from the solution provider directly, we recommend that they insist on knowing what solution the reseller is offering (even if it is 'white-labeled' and offered under the resellers' brand) so that they can become familiar with the underlying service to determine functionality, reliability and sustainability. Again, the focus should be on whether the provider or reseller has sufficient ability to prove legal compliance for electronic notification.

Finally, we excluded providers of solutions that require the recipient of the legal notice to download software or pre-register for an account. Why? We believe, from practical experience, that it is unrealistic to be able to somehow guarantee that the recipient will take compliant action upon receipt of a notice -- action to acknowledge time and content received by, for example, downloading software or registering themselves into a system designated by the sender. One should keep in mind that many recipients will not take the extra time to go through the steps to respond. Indeed, depending on the situation, the recipient might not be permitted to respond and may instead pass a message to an internal process. Further, many recipients put workflow addresses into notice provisions, with the ultimate reader of the message on a corporate computer that is administratively locked down preventing external downloads onto the device.

The technology categories and providers that we considered are:

- **Email:** Microsoft Outlook, VeriSign, RPost
- **Store-and-Forward File Transfer:** Axway
- **Fax:** OpenText

If we had not followed these criteria, we would see a number of additional providers primarily in the Store-and-Forward File Transfer category, as setting up such a system is not complicated. Many newer companies can easily

create a website providing the veil of sophistication, however, their service reliability, security, privacy and sustainability would be hard to determine.

We are only judging those with a full functionality from a single source, rather than companies that might integrate a group of products to 'build' this capability. We believe that "integrated" products often are custom, costly, and not available commercially. If using an integrated product, the customer should use this analysis to ensure the integrator is using product components from the leading companies discussed in this analysis. We have not seen any integrated commercial-off-the-shelf products that would change this analysis.

Therefore, we do not believe including others in the marketplace would change the conclusion of this analysis.

KEY CHARACTERISTICS OF PROVIDERS AND THEIR SOLUTIONS

In this part of the analysis, we have taken the key requirements for strong evidence of compliance with contract notice delivery, and cross referenced these with service providers that meet the criteria noted earlier in this document.

It is important to note that any one of these variables discussed below alone would not likely be sufficient to satisfy evidence requirements. For example, software or services that only provide open tracking have the following limitations:

a. they can only provide information to the sender about opening if the recipient sets their system to return that information, takes some sort of compliant action, or happens to be online while reading the information with standard Internet security settings disabled;

b. they provide no verifiable means to associate the content of a particular message with the record of opening; and

c. typically these open records are presented in simple text that can be easily altered or claimed to have been altered for the benefit of one party or the other.

Practically speaking, and considering the legal definitions of what is deemed the 'time of receipt' of email, **it is not at all practical to rely on an open tracking system for compliance with notice requirements. The recipient can control whether or not and when the email will be shown as having been opened, and without that information, the sender will not be able to prove that that the notice has been 'legally' received.**

This means that the fact that the sender 'sent' the notice at a point in time will have no bearing as to whether or when the notice has been completed or delivered, and open tracking systems will likely not provide any control to the sender as to when or whether delivery has been accomplished. This can have considerable consequences when sending time-dependent notices such as price, service, claims, quantity, specification, delivery, or logistics change orders.

Similarly, most time-stamping services, provide no record of transport – no record of whether or when delivered, but rather focus on time and content of a static document. A record that you had the notice and intended to send it at a point in time will not have much value, as compared to a record of the time the specific notice content was received.

Further, email that has been 'digitally signed' using a PKI digital certificate or that has been 'sender certified' only provides value to the recipient in providing some assurance of who the sender was – or authenticating the sender's origin. These certainly do not provide any information to the sender about whether, what, or when the message was received.

The key characteristics that differentiate the following providers' products or services from standard email, file transfer, or fax are compared as follows:

Provider	RPost	OpenText	VeriSign	Axway	MS Outlook
Product Name	*Registered Email®*	*RightFax*	*Digitally Signed Email*	*Tumbleweed*	*Read Receipt*
Category	*Email*	*Fax*	*Email*	*Store-Forward*	*Email*
EVALUATION REQUIREMENTS					
Delivery Proof	YES	YES			
Open Tracking if Available	YES			YES	YES
Content Proof	YES	YES	YES		
Official Timestamp	YES				
Admissible Evidence	YES	YES	YES		
Functional Equivalence	YES	YES			
Electronic Original	YES	YES	YES	YES	
Self-Authentication	YES		YES		
Portability of Evidence	YES		YES		
Legal Opinion	YES	YES	YES		
Patented Technology	YES			YES	

NOTES AND DEFINITIONS

Delivery Proof – *method of irrefutably proving whether the message was received or failed, without reliance on recipient*
Open Tracking – *provides information on message opening, if available*
Content Proof – *method of proving content of message received*
Official Timestamp – *uniform time stamp cryptographically associated with content*
Admissible Evidence – *meets guidelines on court-admissibility as outlined in case law, if one party challenges the record*
Functional Equivalence – *meets legal guidelines for functional equivalence to traditional methods*
Electronic Original – *method of re-constructing a record and confirming that it is the original content and meta-data*
Self-Authentication – *method of authenticating the record independent of ties to system forensic analysis*
Portability of Evidence – *method of easily transmitting evidence to arbitrator in form that maintains ability to be authenticated*
Legal Opinion – *third-party legal opinion available mapping service/software/methods to the law*
Applicable Patents – *patents issued in at least the United States that are applicable to the evaluation characteristics*

RPost, with its Registered Email® service, appeared to meet all of the criteria noted. RPost states that it has 31 patents issued covering 21 countries relating to third-party authentication of email delivery, content and time.

OpenText, with its RightFax server/service, ranked next, with an electronic fax service. But this solution relies on recipient's providing fax numbers, and may lack robust delivery proof with uniform timestamps, which could present authentication challenges.

VeriSign sells PKI (Public Key Infrastructure) digital certificates that can be combined with email, letting the sender use public key cryptography to "digitally sign" the email. This provides the recipient the ability to verify author and content of the message (although this does not appear to work if the recipient views email in most web-based email programs). However, and importantly, this apparently provides no information about email delivery and no information about timing for the sender, which is likely essential to prove compliance with most contractual notice provisions. Further, there is no uniform timestamp. VeriSign is now a unit of Symantec Corporation.

Axway, with its Tumbleweed store-and-forward service, provides some information about delivery if the recipient takes compliant action and collects the notice by visiting a website to download the file. It does not provide this information in a manner that would have significant evidentiary weight as there is limited verification of delivery and the verification is dependent on action by the recipient.

Microsoft Outlook, with its Read Receipt feature, provides some information about delivery if the recipient sets the option to return the Read Receipt and if the recipient is using a program to read email that is compatible with these read receipts. Similarly, other web-based email tracking services require compliant action (recipient to be online with security settings off) to trigger an open indication. These provide periodic information that would have limited evidentiary weight. This is further discussed in the "open tracking" discussion earlier in this analysis.

SECONDARY CRITERIA

IACCM poll respondents reported ability to minimize administrative time and cost as secondary evaluation criteria. These criteria are covered in the following framework.

Provider	RPost	OpenText	VeriSign	Axway	MS Outlook
Product Name	*Registered Email®*	*RightFax*	*Digitally Signed Email*	*Tumbleweed*	*Read Receipt*
Category	*Email*	*Fax*	*Email*	*Store-Forward*	*Email*
EVALUATION REQUIREMENTS					
User Simplicity	YES	YES	YES	YES	YES
Ability to Automate	YES	YES	YES	YES	
E-discovery Facilitators	YES			YES	
Ease of Implementation	YES				YES
Flexible Cost Models	YES				YES

1. **User simplicity**: Once installed, all have intuitive user interfaces.
2. **Ability to automate**: RPost and OpenText are both easily configurable to send high volumes or automated notices from standard database applications.
3. **Support for compliance with e-discovery**: Of the products analyzed, RPost appeared to have the most robust record for e-discovery and admissibility purposes, along with robust reporting for an administrator. These records are embedded within RPost's Registered Receipt™ transaction record and returned to the sender with an optional on-line secure searchable archive.
4. **Ease of implementation**: RPost and MS Outlook are the simplest to install and implement. RPost states that it integrates with any email program (Outlook, Lotus, Groupwise, Zimbra, BlackBerry, web browsers, etc.), through certain managed email service providers, or as an embedded application within certain appliances. OpenText and Axway require server infrastructure, and VeriSign requires email programs that integrate with PKI digital certificates.
5. **Flexibility in cost models**: In terms of pricing and plans, RPost has opted to provide services either on a pay-per-use basis with pricing published on its website (with all software, start-up, service, support, training cost fully loaded into a cost equivalent to about the cost of a postage stamp per use), or unpublished per user monthly or annual licenses. The others do not have pay-per-use plans and generally obscure pricing specifics.

REQUREMENTS SCORECARD AND CONCLUSION

A score is often a useful measure to address the extent of the differences among these service providers and the notice methods. The following requirements summary chart references the evaluation criteria above, scoring each on a scale of 3 to 1, with 3 being the highest score.

Provider	RPost	Verisign	OpenText	Axway	MS Outlook
Product Name	***Registered Email®***	***Digitally Signed Email***	***RightFax***	***Tumbleweed***	***Read Receipt***
Category	***Email***	***Email***	***Fax***	***Store-Forward***	***Software***
Evaluation Requirements					
Delivery Proof	3		1		
Open Tracking	3			2	2
Content Proof	3	3	1		
Official Timestamp	3				
Admissible Evidence	3	3	2		
Functional Equivalence	3		2		
Electronic Original	3	3	2	2	
Self-Authentication	3	3			
Portability of Evidence	3	3			
Legal Opinion	3	3	3		
Patented Technology	3			3	
User Simplicity	3	1	3	3	3
Ability to Automate	3	1	3	2	
E-discovery Facilitators	2			2	
Ease of Implementation	3				3
Flexible Cost Models	3				3
Total	**47**	**20**	**17**	**14**	**11**

The RPost service satisfied the evaluation requirements with a score that was more than double the score of the closest comparable technology and service provider. More importantly, RPost was the only solution that satisfied all seven legal requirements essential to yield a legally valid and court admissible record with high evidential weight as to the official time a notice was sent, received, and the content of the notice cover and attachments. This protects the sender's organization in the case where time, receipt, notice content, or notice compliance is challenged by the recipient.

The RPost service is the provider of choice for converting legal and contract notices to electronic delivery. Additionally, the RPost service includes advanced email encryption options and functionality for obtaining recipient electronic signatures on contracts attached to email, as an all-in-one package.

1900 Avenue of the Stars, 7th Floor
Los Angeles, California 90067
310.203.8080—(fax) 310.203.0567

Two Embarcadero Center, 5th Floor
San Francisco, California 94111
415.398.8080—(fax) 415.398.5584

3 Park Plaza, Suite 1100
Irvine, California 92614
949.623.7200—(fax) 949.623.7202