Email Encryption Services Buyers' Guide

2011 Update

Presented by
Frank Sentner
Director of Technology
The Council of Insurance Agents & Brokers

THE COUNCIL
The Council of Insurance Agents & Brokers

Abstract

This paper has been developed in response to The Council members' requests for guidance on which email encryption service would best help them comply with heightened regulations regarding email encryption in certain circumstances. This paper will assume The Council members have themselves, with counsel, identified which communications should be transmitted in encrypted form to comply with HIPAA regulations in the United States, FSA requirements in the United Kingdom, or other requirements that they may have identified.

Why is this important now? There is a recent dramatic expansion of HIPAA's regulatory net. Email encryption is the best method of complying with data privacy rules. The Council's members report the marketplace for email encryption services has become sufficiently complex to evaluate; the vendor selection process is complex.

This analysis has been reviewed and tested by The Council for accuracy. The Council interviewed member firms using the email encryption vendors discussed in the analysis, to confirm accuracy of the analysis results. From this review The Council believes the framework and results are a fair and useful representation of the marketplace, based on publicly available information.

In 2010, The Council reported its top technology pick in its Email Encryption Buyer's Guide as RPost. The Council has established a fee arrangement such that RPost now contributes a portion of fees collected from members to The Council. Such non-dues revenue is useful for The Council to keep member dues costs low. As the top pick in the 2010 Guide, The Council also asked RPost to contribute technical expertise and marketplace insight to the preparation of this comprehensive email encryption marketplace analysis.

This analysis has been provided for information only. The Council does not provide legal advice and disclaims any liability due to any party's reliance on this analysis for selection of any particular software. The Council has based this analysis on publicly available information and disclaims the accuracy of such publicly available information. For recommendations to your specific circumstances, please consult your own legal and technical consultants.

Frank Sentner, Director of Technology at The Council of Insurance Agents & Brokers

July 2011

Whitepaper Contents

Important New Considerations

In The Council's 2010 Buyer's Guide to Email Encryption Services, we identified top level and secondary criteria to examine when evaluating and comparing encryption service provider offerings.

In this 2011 update, we focus on new considerations and an expanded set of top level purchase drivers listed in order of importance, some of which re-affirm and update the importance of the purchase drivers and discussion from the 2010 analysis.

With heightened enforcement actions by regulators, the purchase driver of email encryption services is no longer whether or not the provider's solution is 'secure enough' but is now how well the provider's solution will protect from fines in the case of a data breach.

All of the vendors discussed in this guide have systems that are 'secure enough' to comply with security 'best practices' and regulator guidelines for encryption. Further, customer IT departments can select various methods of making these encryption services available to senders, with all of the vendors discussed having options for sending encrypted ad-hoc via a desktop plug-in or key word insert, or auto filtered by policy at the outbound gateway -- thereby making the sender experience equally simple across each of these discussed vendors. Therefore, these points are not the focus of our analysis. What we will focus on, as top level evaluation criteria, is **how well the solutions will protect from fines in the case of a data breach**.

When considering data breach, we are considering two points, a data breach when the data is (a) **within the sender's control** (i.e. where the email is sent from sender to recipient - "sender-controlled data security"); and (b) **after the data leaves the sender's control** (i.e. if there is a data breach on the recipient's system or after the recipient forwards the information on to others - "downstream data breach").

Reducing risk when data is within the sender's control is a function of how and how often users use the email encryption service. Data and visibility into use patterns, training gaps, policy effectiveness, elegant and simple user interfaces, service breadth, and simplicity of the user experience all contribute to reducing risk of a data breach when the protected data is within the sender's control, as the service is used, used more, and this usage can be monitored and confirmed.

Reducing risk after data leaves the sender's control is a function of visibility and ultimately proof that the sender has complied with data privacy requirements. This proof should stand up to the test of litigation or government audit even in the case where the sender is accused of contributing to a data breach. In this guide, we call this auditable proof of compliance.

We have considered the above in developing our new list of recommended top level purchase drivers for email encryption services, and we rank each provider on a scale of 1 to 3 in each category, with 3 being the highest score.

Purchase Drivers

The following are the results of a poll conducted in July 2011 that included 65 member company representatives.

1. Besides 'compliance', the most important benefit of email encryption services reported by respondents is to create new administrative efficiencies (75%) followed by cost savings (19%) and then paper reduction (6%).

2. Half of respondents polled are sending sensitive or protected data today, using email encryption services of some kind (55%) with half of those respondents satisfied with their current service (54%) and one third unsatisfied and looking to change (31%).

3. Adoption of email encryption services by those not using such services today will likely bring first risk reduction, as those respondents not sending sensitive and protected data using email encryption services reported primarily sending the information by standard email (18%). The next benefit is likely administrative efficiencies as 13% reported using fax. Cost savings and paper reduction would occur, but as a lower benefit as only 10% reported using standard mail and 5% reported using expensive courier/receipt mail.

This analysis focuses on three categories of purchase drivers.

Importance Rank 1: Enterprise Security Intelligence
Importance Rank 2: User Simplicity
Importance Rank 3: Breadth of Offering

Considering these purchase drivers as described in this analysis, members ranked Enterprise Security Intelligence and User Simplicity and higher than Breadth of Offering.

As in the 2010 analysis, for this analysis, The Council is only considering for its recommendation those solution providers that have developed and operate the technology, and not those firms that resell a technology solution from one of the companies listed below.

Assuming that Council members would prefer to implement technology that has proven sustainability in the marketplace, we have focused this analysis on only those providers who have been servicing commercial enterprise customers for more than 5 years. If members are considering purchase from a reseller rather than from the solution providers directly, we recommend that they insist on knowing what solution the reseller is offering, even if it is 'white-labeled' and offered under the reseller's brand, to use this analysis as a decision tool. Finally, the providers selected and listed below have been evaluated from the point of view that Council member firms will prefer to not require their email recipients to download software or pre-register for an account with a solution provider.

Solution Providers	
RPost	***"Encrypted Delivery Direct"*** *– With this system, the recipient receives the encrypted data right in their inbox, the recipient does not have any requirements to be online to decrypt or view the message, and there is no storage of message content by RPost.*
Voltage **Cisco Ironport** **Zixcorp**	***"Store-and-Forward"*** *– With these, the systems either store the message content and/or the encryption key in an online repository. If the key is stored online, then the systems permit delivery of encrypted data to recipients' desktops,* ***with a required multi-step recipient pre-registration process*** *and a recipient requirement to be online for a 3-step data decryption web service exchange to decrypt the message in the inbox.*
Axway Tumbleweed	*"**Link Retrieval**" - With this system, a secure file transfer system, the recipient must register and arrange for a password exchange. Further, the recipient must be online to retrieve and download the message.*

Service providers, such as Google/Postini, Symantec/Messagelabs, AppRiver, Sendmail, Microsoft, among others, private label or resell solutions from some of the above companies. Newer service providers are not evaluated here due to a risk of inexperience in being able to service enterprise customers and risk of sustainability in the marketplace.

Scorecard

The following scorecard is a useful quick reference comparison that is discussed in detail in the following analysis. With this quantitative approach, **RPost ranks with a score that is nearly double the closest comparable.**

Scorecard: Evaluation Criteria

Scoring: 3 is high, 1 is low

Rank	Top-Level Purchase Drivers	RPost	Cisco Ironport	Axway-TMWD	ZixCorp	Voltage
1-	**Enterprise Security Intelligence**	**11**	**5**	**6**	**5**	**2**
	Auditable Proof of Compliance	*3*	*1*	*1*	*1*	*0*
	Optimization Reporting	*3*	*1*	*1*	*1*	*0*
	Electronic Discovery and Data Access	*2*	*1*	*2*	*1*	*1*
	Visibility	*3*	*2*	*2*	*2*	*1*
2-	**User Simplicity**	**8**	**7**	**5**	**5**	**6**
	Recipient User Experience	*3*	*2*	*1*	*1*	*2*
	Recipient Workflow Addresses	*2*	*2*	*2*	*2*	*2*
	Sending Automation	*3*	*3*	*2*	*2*	*2*
3-	**Breadth of Offering**	**9**	**5**	**5**	**5**	**5**
	Sender Apps	*3*	*1*	*1*	*1*	*1*
	Breadth of Features	*3*	*1*	*1*	*1*	*1*
	Configuration Flexibility	*3*	*3*	*3*	*3*	*3*
	SCORE	**28**	**17**	**16**	**15**	**13**

The Council's Recommendation: RPost (www.rpost.com/secure)

The Council's top recommendation is once again, RPost. RPost recently upgraded its SecuRmail™ service. RPost has demonstrated its ability to continuously innovate at a rapid pace and at the request of members to fulfill specific needs, to respond to market needs, and to enhance its solutions with well thought out and often unique implementations. RPost announced in June a major service upgrade which addressed key points of interest for our members as described in the chart below. Further, RPost has engaged in a quality drive for its services and support which members report as being successful. **Finally, RPost has been built into and/or configured for compatibility with the largest insurance agency management systems and the most common mobile messaging devices.**

RANK 1: Enterprise Security Intelligence

Gartner research has identified an important and necessary next step in enterprise security, which Gartner analyst Joseph Feiman has coined "enterprise security intelligence." In Feiman's research, entitled, "Prepare for the Emergence of Enterprise Security Intelligence," Feiman describes enterprise security intelligence as a comprehensive approach to enterprise security that enables advanced security through improved analytics leading to optimal decision making. Security activities, and the information that results from them, can no longer be considered in isolation. Mature enterprise security requires interaction and correlation of different security technologies to increase accuracy and breadth of security detection, remediation and protection. It also requires the integration and correlation of security and contextual information to bridge security with business, risk and other key enterprise values, thereby enabling optimal decision making.

We agree with Gartner that a missing link in many security initiatives is robust reporting that can be analyzed in a manner that provides greater intelligence for technology and security staff so that they can adjust, react, and improve security software, settings, and activities. We now believe this is an element that ultimately may reduce risk and thus better protect members in cases of security audits, can empower more effective training, can test policy effectiveness, and can ultimately protect against losses and fines associated with security and data privacy breaches.

More specifically, in the context of members' businesses, we identify four areas of enterprise security intelligence that we believe should be considered essential: (a) Auditable Proof of Compliance, (b) Optimization Reporting, (c) Electronic Discovery Access, and (d) Visibility. It is these aspects of enterprise security intelligence that encompass our top rank as the most essential evaluation item in purchasing an email encryption service.

A. Auditable Proof of Compliance

Probably the most important element to test in your email encryption service that will protect you from fines in the case of a data breach is how robust the proof record is of the fact that certain data was sent and received in a compliant manner. We call this **protection from downstream data breach.**

Consider the following:

1. You send an email encrypted with an attached document,
2. The document contains protected health information,
3. The document is on your letterhead or otherwise shows it originated from you,
4. The recipient forwards the email and/or document, or otherwise exposes the information (inadvertently, through unauthorized access to their system, or otherwise), to an unauthorized party. There is a claim of a data breach or HIPAA violation,
5. Fines are threatened, and, as the document is on your letterhead, you are implicated.

How do you irrefutably prove that you sent that document encrypted to the recipient and the data breach happened after the document left your realm of responsibility? How do you do this before costs ramp up – costs for lawyers, technical experts, and forensic experts?

There are common misconceptions that the following items will protect you from fines associated with the data breach. They likely will not.

1. **Text server logs:** These can be hard to locate, associate to the content and can be easily challenged after the fact (days, weeks, or months later). It can be difficult / expensive to (a) find these logs, especially if the message was delivered by an email provider outside of your realm, (b) irrefutably associate the logs with specific message content and timestamps, and (c) prove the text files are authentic when authenticity is challenged.
2. **Sent item records:** These will often show the content originated in your organization, but will likely not demonstrate the fact *if* the message was transmitted and successfully received, *what* was received and *when*, or whether it was received encrypted.
3. **Archive services:** These often tout logging all items sent and received. However, in most cases, this does not relate to the same message. Archive services are not logging a SPECIFIC message's path of sending and whether or not that message was received by the recipient; rather, they are logging that a message (often without any easy method to associate message content) has been sent and separately, they log that if a message has been received. To be clear, this is not logging that the message in question has been sent AND received by the intended recipients, but only half of the activity – that the message has been claimed to have been sent.

What is needed is a record of precisely what message content was in fact sent and then later received by each intended recipient <u>in an encrypted manner</u>.

It seems that only RPost has a robust mechanism in place to provide an auditable record of precisely what message content (body text and attachments) was in fact sent and received in an encrypted manner to each intended recipient. This is important because, in the case where there is a data breach after the email has reached the recipient (in the recipient's environment, or after they have passed the information along to

others), the sender will need to retain information to prove that the breach did not happen "on their watch" – that they in fact complied with the data security requirements and delivered the information in a compliant, encrypted manner.

RPost addresses this issue by having built its encrypted email service on top of its core Registered Email® service, which The Council endorsed in 2004 as the best way to prove email content, time, and delivery with court-admissible records that can be authenticated. By doing this, RPost provides not only effective encryption, but also the most robust proof and record of compliance with the rules of regulators.

We believe this is an important (and often overlooked) evaluation criterion, especially considering that Council members have placed a high value on encrypted email services fulfilling the need to **protect them from fines in the case of a data breach.**

We recommend that you avoid services that do not have a robust audit trail of delivery that can be independently verified as to encrypted delivery, message content, have independent timestamps that are not based on sender/recipient desktop or server times, and avoid reliance on text logs or web screens of transaction audits.

B. Optimization Reporting

A problem that many face is they deploy email encryption services, yet they have very little visibly into how these services are being used, whether they are being uses, who is or is not using them, and if they are being used, in reasonable/appropriate (pick one) quantities as a percentage of overall email traffic.

We recommend looking for services that provide intelligence around use of the security / email encryption services so that you can:

a. Identify training gaps and adjust accordingly
b. Consider whether usage patterns by certain groups are at appropriate levels based on the type of business those groups engage in
c. Test effectiveness of content filtering policies, and
d. Optimize enterprise user and use licenses based on message volume or identified user.

Of the providers identified for this analysis, Zix, Ironport, and Tumblweed provide some information as to whether or not recipients happen to download messages posted to message centers, but this information is limited and sporadic and relies on the fact that the recipient must collect the message. Voltage does not appear to provide any reporting whatsoever. RPost appears to have the most advanced reporting. RPost provides advanced reporting in both CSV and XML formats that can parse into enterprise business intelligence systems to provide the IT organization with message-level and user-level statistics on each encrypted transmission. This assists IT staff in optimizing content filtering policies and end-user training priorities, increasing security across the organization.

C. Electronic Discovery and Data Access

It is important to have a mechanism in place to have protected data stored in an encrypted manner, yet be easily accessible in case of a need to produce information in an electronic discovery situation arises.

Challenges here are:

1. If documents are uploaded (or transmitted from the desktop using HTTPS vs SMTP) to a web-based message store for transmission of a download link to the recipient, that document may not be stored in the messaging archive as the HTTP upload would have bypassed the email messaging archive. Also, typically a message is not stored by a web based message store for more than a short period of time and therefore could pose a risk proving the content of the message after that time frame.

2. If messages are encrypted at the mail gateway, they remain unencrypted within the sender's organization, are captured in the messaging archive, but are captured in an unencrypted view that leaves vulnerability in terms of access to protected data. Further, in terms of electronic discovery needs, the archive will retain a record of what was claimed to have been *sent*, but will not likely have any information related to *delivery* or third-party uniform timestamps to confirm time of receipt.

3. If messages are encrypted at the desktop of the sender and routed out encrypted, there are not issues identified with points (1) and (2) above, yet message archive systems will retain or save the encrypted message. The sending organization will need a later method of decrypting those archived encrypted messages should it be necessary or required.

In your evaluation, consider which providers have thought through their products enough to consider these. With:

a. Desktop encryption: avoid service providers that do not have a robust mechanism to retrieve and decrypt stored encrypted messages.
b. File upload services: avoid service providers that offer these services without robust records of the messages uploaded, otherwise you expose your organization to data leaks and accusation of data leaks without ability to track message transmission.
c. Gateway/Appliance: avoid service providers that send encrypted data without robust and verifiable delivery reporting records.

D. Visibility

When sending email encrypted, it is important (a) for the sender to know (and have confidence) that the message was transmitted encrypted, and (b) that the recipient know that the message received was transmitted encrypted, regardless as to whether or not TLS was used for encrypted transmission on the recipient side.

Why?

For the sender (or sender organization), they need the confidence of knowing that their email encryption service is working or functioning properly. For example, consider what happens if a sender (or sender risk or

IT security department) believes they are sending email encrypted and that encryption will happen automatically at the sender's gateway based on some indication in the message. What if that filtering mechanism is not working properly for whatever reason? Most senders with most appliances/filters may have no way of knowing immediately when the filter stops working properly – each day of improper function may causes escalating risk of fines associated with data breach regulations.

For the recipient, they need to become aware that the sender has flagged that particular message content as sensitive, and thus have some knowledge that the message should be treated as such – sensitive and protected.

Consider what happens if TLS routing is preferred for the secure transmission to the recipient, yet a TLS routed message received by the recipient looks just like a normal email. And, most senders that add boilerplate disclaimers on the bottom of emails add to all emails so as not to differentiate from those that contain protected data and those that do not. This lack of awareness by the recipient creates the potential for inadvertent forwarding or treatment of the protected information.

All of the email encryption providers – with the exception of RPost - seem to have missed these important points. RPost does provide the sender the security intelligence – in the form of a Registered Receipt email on a message by message basis, as well as with daily, weekly, or monthly user and enterprise reporting. Further, RPost formats the message so that - whether the message is encrypted to the recipient desktop or routed via TLS encryption - the recipient becomes aware that that message either contains an encrypted file or was transmitted via an encrypted transmission protocol. This awareness for the recipient reduces overall risk.

Rank 1 Vendor Score: RPost ranks highest in each of the four elements of enterprise security intelligence. Second is Axway Tumbleweed, Cisco Ironport and Zix tie for third, and Voltage ranks fourth.

Scoring : 3 is high, 1 is low

Rank	**Top-Level Purchase Drivers**	**RPost**	**Cisco Ironport**	**Axway-TMWD**	**ZixCorp**	**Voltage**
1-	**Enterprise Security Intelligence**	**11**	**5**	**6**	**5**	**2**
	Auditable Proof of Compliance	*3*	*1*	*1*	*1*	*0*
	Optimization Reporting	*3*	*1*	*1*	*1*	*0*
	Electronic Discovery and Data Access	*2*	*1*	*2*	*1*	*1*
	Visibility	*3*	*2*	*2*	*2*	*1*

RANK 2: User Simplicity

If email encryption systems are cumbersome, there is less use and therefore, potentially more exposure to a data breach.

All of the systems evaluated have simple methods of sending. The focus in this section evaluates the simplicity of the recipient user experience, and some other aspects.

There are a variety of modes that these service providers offer as methods of implementing that can alter the recipient user experience. In general, we break the service providers into three categories, focusing on the differentiating elements among the service providers.

Encrypted Delivery Direct: With this system, the recipient receives the encrypted message content right in their inbox, with the message embedded in an AES 128 or 256 bit encrypted PDF wrapper. The recipient does not have any requirements to be online to decrypt or view the message, and there is no storage of message content by the service provider, in this case, RPost. The message body text appears in PDF format, while all attachments remain in their native file format.

Store-and-Forward: The service providers either store the message content or the encryption key in an online repository; then later forward it to the recipient in a specific process. If it is the key that is stored in the online, then the systems permit delivery of encrypted data to recipients' desktops, with a required multi-step recipient pre-registration process and a recipient requirement to be online for a 3-step data decryption web service exchange to decrypt the message in the inbox. When the recipient receives the encrypted message content in their inbox, the message is embedded encrypted within an HTML file wrapper. Again, the recipient does have to be online to decrypt or view the message, and there may be message storage by the service provider. Zix, Voltage, and Cisco Ironport operate in this manner.

Link Retrieval: With this system, essentially a secure web file transfer system, the recipient must register and arrange for a password exchange. The recipient must be online to retrieve and download the message. The security is arranged through a secure web protocol connection.

The 'store-and-forward' or key-retrieval email systems require the recipient to take meaningful or significant action for the recipient to retrieve the email – often clicking through to a website, setting up an account with the provider, installing software plug-ins on the recipients' computer, which typically is not allowed without the recipient having administrative rights (rare in corporate environments), and then downloading the message to their desktop. We have heard from insurance brokers that these systems are challenging due to the low response rate for clicking through to download the material. Some of these store-and-forward systems require recipient registration for a more seamless experience, but in reality, if there are hurdles to getting the information to the recipient, the fallback is unfortunately for the sender to re-send the email unencrypted. Therefore, we conclude that there is greater risk of a data breach or fines with these "store-and-forward" systems.

By contrast, RPost delivers the encrypted material right to the desktop without a requirement for the recipient to be online to decrypt and read the message, reducing risk as compared to the other providers. This is a unique element of the RPost system.

In addition to simplicity for general senders and recipients, one should also consider the following:

1. **Simplicity for recipient workflow addresses:** If the senders are sending to recipient addresses that are recipient generic workflow mailboxes (i.e. claims@insuranceco.com), the email encryption service providers should consider how to deliver to those workflow addresses that make it easy for multiple recipients that have authorized access to that address to decrypt the messages. All of the providers have mechanisms to simplify this process that are different but equally effective.

2. **Automation:** There are two considerations in terms of automation, (a) automated filtering messages by policy and auto routing for encryption, and (b) automated sending of batches of emails with encryption. All of the providers in this analysis have mechanism for automated content filtering and routing for encryption. RPost is best suited for automated batch sending of messages with both web services APIs and SMTP message format options.

Rank 2 Vendor Score: RPost ranks highest in all elements of user simplicity. Second is Cisco Ironport, followed by Voltage and then Zix and Axway Tumbleweed.

Rank	**Top-Level Purchase Drivers**	**RPost**	**Cisco Ironport**	**Axway-TMWD**	**ZixCorp**	**Voltage**
2-	**User Simplicity**	**8**	**7**	**5**	**5**	**6**
	Recipient User Experience	*3*	*2*	*1*	*1*	*2*
	Recipient Workflow Addresses	*2*	*2*	*2*	*2*	*2*
	Sending Automation	*3*	*3*	*2*	*2*	*2*

RANK 3: BREADTH OF OFFERING

Consider in this category, a service provider's offerings in terms of breadth in:

A. **Sender Apps:** seamless methods of using email encryption services as extensions to existing email offerings, embedded within sender email applications such as Microsoft Outlook and others.

B. **Breadth of Features:** With renewed interest in electronic signature efficiencies, consider providers that combine, on a message-by-message basis, HIPAA compliant encryption with other services such as HIPAA compliant secure electronic contract execution, standard message (unencrypted) delivery proof, and other security related features are a bonus.

C. **Configuration Flexibility:** There are several common user modes that can be enabled, designated by sender, user group or organization. Offering these user modes expands the flexibility of implementing email encryption offerings.

    1. Encrypts the message locally at the sender's desktop or mobile device, ensuring encrypted delivery straight through to the recipient's desktop; securing from the potential of data breaches both within the sender's in-house or outsourced email system, and external while in transport across the Internet and within the recipient's email system.
    2. Encrypts the message at least from the edge of the sender's network to at least the edge of the recipient's network. This permits corporate filtering functions to continue to scan email within the sender's or recipient's organization.
    3. Automatically encrypts messages at the sender's outbound mail gateway based on message content or other criteria.
    4. Permits the recipient the ability to ad-hoc reply secure is a configuration that is important to create a secure community, or for secure collaboration.
    5. Permitting customers start with a pay-per-use basis to evaluate user and usage patterns, and then convert to pay per user pricing. This helps members optimize cost and user licenses.
    6. Most are relatively easy to implement, especially those that do not require appliances or gateway servers.

Rank 3 Vendor Score: RPost ranks highest in terms of service breadth with the most options in terms of sender apps and additional important features. All of the providers offer somewhat flexible configurations with RPost providing the most flexible pricing as noted in C5 above. RPost provides seamless methods of using email encryption services within sender email applications including Microsoft Outlook, Lotus Notes, Apple email products, Microsoft Hotmail, Yahoo, Gmail, BlackBerry, among others. RPost also offers API's for developers to tie RPost secure messaging services into their enterprise email applications or automated processes. Of note, **RPost mobile apps** encrypt messages at the sender's mobile device and delivers encrypted to the recipients' desktop or email account, whether or not they are on the same telecom network. RPost has apps for BlackBerry, iPad, iPhone with others said to be released in 2011.

In terms of breadth of features, with RPost, users can combine, on a message-by-message basis, RPost encryption with other RPost services with a few extra clicks and at no extra cost. These additional services include Registered Email legal delivery proof, sender authentication, official time stamping, message content authentication, attachment PDF conversion and meta-data cleansing, large file transfer, secure (HIPAA compliant) electronic contract execution, records and matter management, message subject line tagging, and e-discovery options for special auto-routing of message records.

Rank	**Top-Level Purchase Drivers**	**RPost**	**Cisco Ironport**	**Axway-TMWD**	**ZixCorp**	**Voltage**
3-	**Breadth of Offering**	**9**	**5**	**5**	**5**	**5**
	Sender Apps	*3*	*1*	*1*	*1*	*1*
	Breadth of Features	*3*	*1*	*1*	*1*	*1*
	Configuration Flexibility	*3*	*3*	*3*	*3*	*3*

Conclusion

The Council's top recommendation is once again, RPost. RPost recently upgraded its SecuRmail™ service. RPost has demonstrated its ability to continuously innovate at a rapid pace and at the request of members to fulfill specific needs, to respond to market needs, and to enhance its solutions with well thought out and often unique implementations. RPost announced in June a major service upgrade which addressed key points of interest for our members as described in the chart below. Further, RPost has engaged in a quality drive for its services and support which members report as being successful. **Finally, RPost has been built into and/or configured for compatibility with the largest insurance agency management systems and the most common mobile messaging devices.** More information about RPost can be found on their website at **www.rpost.com/secure**.


THE COUNCIL
The Council of Insurance Agents & Brokers