CYBER SECURITY & COMPLIANCE BUYER'S GUIDE

For Real Estate Services Providers

RESPRO GOLD STANDARD
SECURITY & COMPLIANCE

RESPRO®
Real Estate Services Providers Council, Inc.

The **Real Estate Services Providers Council®** (RESPRO®) has developed this Cyber Security and Compliance Buyer's Guide to assist its members and those operating in all sectors of the residential real estate market manage risks associated with data breaches, consumer information privacy, and compliance with TRID notice and consent rules.

This Buyer's Guide compares vendors and technologies in different categories, identified by RESPRO® members when considering solutions to comply with consumer privacy laws and the TILA/RESPA Integrated Disclosure (TRID) rules, while keeping the residential real estate transaction process simple and streamlined.

RESPRO® developed this Buyer's Guide with data gathered from interviews conducted with its members, assessments of existing IT vendors, and analysts' insights. The Guide includes detailed reviews and comparisons of technologies and providers offering services for:

- **Email Encryption** for privacy, for both security and compliance with rules protecting consumer Nonpublic Personal Information (NPI).
- **E-Delivery** Proof for proving TRID (TILA-RESPA Integrated Disclosure) time-dependent notice delivery compliance, and other required notices.
- **E-Signatures** for recording proof of consent to use electronic signatures and designated email addresses in a transaction (for ESIGN and UETA compliance), and for productivity enhancements through instant electronic execution of transactional documents and forms.

RESPRO® is a national non-profit trade association with members touching the majority of residential real estate transactions in North America.

CONTENTS

I. Executive Summary 5
Introduction 5
Summary Conclusions 7
Gold Standard Endorsement 9
Why RMail as the Top Choice for Email Encryption (for NPI Privacy Compliance) 9
Why RMail as the Top Choice for E-Delivery Proof (for TRID and Other Notices) 10
Why RMail As the Top Choice for Legal E-Signatures (to Record Consumer Consent) 10
II. Analysis: Email Encryption for Privacy and Compliance 13
Email Encryption Solutions Evaluated: 13
Evaluation Criteria: 14
1. Compliance and Security Intelligence 14
2. User Experience 17
3. Breath of Offering with Required Features 18
4. Weighting Top Level Criteria 19
Email Encryption – Solution Scorecard: 20
Table: Email Encryption Solution Scorecard 20
III. Analysis: Electronic Document Delivery for TRID Compliance 22
E-Delivery Solutions Evaluated: 22
Evaluation Criteria: 23
1. Compliance & Auditable Proof 23
2. User Experience 26
3. Breath of Offering with Required Features 27
4. Weighting Top Level Criteria 28
E-Delivery Proof – Solution Scorecard: 29
Table: E-Delivery Proof Solution Scorecard 29
IV. Analysis: Legal Electronic Signatures to Prove Consent 31
Investor Criteria 31
RESPRO® Top Level Evaluation Criteria 32

E-Signature – Criteria Rating: 33
V. RESPRO® Evaluation Highlights 35
RMail® Encryption (for Security and NPI Compliance) 35
Compliance & Security Intelligence 35
User Experience 36
Breadth of Offering with Required Features 36
RMail® Track & Prove Service (TRID and Notice E-Delivery Compliance) 36
Verifiable, Durable and Portable Record Authentication 36
RPost® E-Signature Services (Recording Consent and Agreement) 38
I. RPost E-Signature Foundational Elements 38
II. RPost E-Signature Differentiated Elements 39
RESPRO® Endorsement Summary 40
VI. Registered Receipt Record as Uniform Proof of Compliance 42
Registered Receipt 42
Structure of the Registered Receipt™ Record 43
Legal Proof of Delivery 43
Protocol Level Transmission Meta-Data 45
Verification of a Registered Receipt Record 47

1

EXECUTIVE SUMMARY

I. EXECUTIVE SUMMARY

Introduction

With all aspects of real estate transactions migrating to faster and more efficient digital processes, new laws and regulations are catching up to protect consumers with regards to these transactions. In parallel, new cyber security threats have created a new dimension of financial risk.

The combination of these market forces has led RESPRO® to support members in evaluating technologies that not only meet perceived cyber security and compliance requirements, but also focus on using best practices to ensure top level protection, maintain systems to prove compliance for use in an audit, examination, insurance claim, or legal action, and continue a drive for productivity though technology.

Data breaches and lack of proof of compliance with disclosure requirements can impact RESPRO® members far beyond simple fines. Additional risks include:

- ☐ Cost of holding loan principal caused by inability to prove disclosure compliance, sufficient to transfer the loan;
- ☐ Reputational damage arising from disclosure of the data breach;
- ☐ Lawsuits from clients, consumer privacy advocates, or others impacted by a data privacy breach;
- ☐ Financial loss due to cyber-criminals intercepting email correspondence causing consumers to divert closing funds to imposter bank accounts; and
- ☐ Class action lawsuits claiming insufficient disclosure or consumer privacy protection.

In terms of security and consumer information disclosure, business practices and regulatory pressures are pushing real estate services providers (agents, brokers, lenders, settlement agents, title companies, and others in the integrated business of residential real estate) toward solutions to protect private information. Criminal acts are creating urgency as well.

The trend in increased security concern is highlighted by increasingly common fraud schemes, such as one where hackers intercept emails from title, escrow and closing agents and/or use social engineering to carefully forge emails. In these schemes, the hacker or imposter hijacks back-and-forth communications ending in the supply of fake wire transfer information sent to the home buyer. In this scheme, the unsuspecting consumer then wires their down payments directly to the disguised account which routes

the consumer funds to the cyber-criminal's bank account overseas. The funds are lost forever. The transaction is mired in chaos and blame.

The fraudulent emails often appear genuine and contain the text, writing style, branding, first names of the agents and other parties, and/or email addresses that make the emails appear as a legitimate part of the real estate closing.

- The FBI refers to the above email scam as "Business Email Compromise" scheme and estimates that imposters have used these tactics to scam 7,000 victims, taking in average increments of $6,000 from individuals and $130,000 from businesses, for a total of nearly $750 million stolen in the United States alone, between October 2013 and August 2015.
- RESPRO® is aware of this scheme being used to intercept funds during the real estate closing process and in other parts of business interaction.

RESPRO® believes email encryption and certified e-delivery tracking and proof are tools that can mitigate these risks. The industry as a whole is moving in this direction.

- Gartner, the world's leading information technology research and advisory company, identifies in its *Market Guide for Email Encryption* main trends for more use of email encryption, including: growth in digital business, heightened regulation, and revelations of nation state surveillance activities.
- RESPRO® members are likely to have risks that cut across their integrated business units and affiliated companies. As such, risks may be much greater for members. According to the Ponemon Institute, a pre-eminent research firm dedicated to privacy and data protection, for larger companies, the most expensive cyberattack experienced and reported in their study incurred more than $51 million in damages and remediation costs; while the smallest was still more than $1 million. The average expenditure to remediate these attacks was $7 million. Ponemon Institute also reports that among 350 companies surveyed, the average cost of a data breach was $3.8 million.

On the compliance side, the mortgage, real estate, title insurance, consumer lending, and legal industries are facing the most comprehensive changes in federal mortgage disclosure requirements in more than 30 years. To maintain and prove compliance with

the Consumer Financial Protection Bureau (CFPB) TRID e-delivery rules and to retain proof of protection of consumer nonpublic personal information (NPI) as required by the Gramm-Leach-Bliley Act (GLBA) in case of a claim of a data breach, RESPRO® members should only exchange documents, data and information with attorneys, real estate brokers, lenders, title insurers, settlement agencies, partners, and clients using certified e-delivery proof; with encryption when transaction details are included.

RESPRO® analyzed technologies and solutions focused on the three most important areas of concern for members -- email encryption, certified e-delivery proof for TRID compliance, and e-signatures to record consent in a form acceptable to loan investors and as defined by ESIGN and UETA. In this Buyer's Guide, RESPRO® presents its findings and recommendations to members.

Summary Conclusions

Through RESPRO®'s analysis, **RESPRO® has identified one solution, RMail® by RPost®, that stands above the rest.** RMail (www.rmail.com) by RPost is exemplary not only because it meets member needs for email encryption, certified e-delivery proof, and e-signatures at the highest levels, but also because it includes all of these and more, in a simple to use, all-in-one offering.

Foundational elements of the RESPRO® endorsement of RPost services are the Registered Receipt™ email record and RPost's ability to innovate to adapt its product to changing market needs.

- Registered Receipt Auditable Proof: This Registered Receipt record is the uniform transaction record returned to the sender for each processed message. It returns the a high evidential level of proof --- verifiable, durable, and auditable proof of compliance with data privacy, e-delivery, and e-signature requirements.
- Innovation: RPost includes a new "anti-whaling" feature to detect "whaling" attacks that otherwise lure transaction participants into wiring closing funds to bank accounts controlled by Internet criminals.
    - Internet criminals have been attempting to intercept escrow funds after receipt of funds by the closing escrow agent.
    - Now, these Internet criminals are also attempting to intercept escrow funds before they reach the escrow agent.

- These Internet criminals use advanced research to identify home buying service providers and participants in the transaction and then correspond with certain transaction participants who have the authority to transfer funds, with the Internet criminal masquerading as a known person of authority involved in the transaction.
- After gaining trust with back and forth correspondence, the Internet criminal lures the escrow / closing agent or home buyer into sending down payment funds to a disguised bank account controlled by the Internet criminal. As none of the correspondence ever originated with authentic participant involved in the transaction, no one is aware of the risk or fact of funds having been diverted. In most cases, no one realizes funds have been intercepted until a few days later when everyone is asking about the closing funds. At this point, the transaction is mired with chaos and closing funds have been diverted to a foreign account of the Internet criminal, and are irretrievable.
- The FBI calls these attacks "Business Email Compromise" and the technology industry calls them "whaling" attacks, a form of “phishing”.
- After identifying the seriousness of the abovementioned issue for RESPRO® members through discussions with RESPRO® board members and their staffs, RPost teams implemented new, patent pending security into RMail; security that includes advanced algorithms to identify and warn email users when these “whaling” attacks are being attempted.
- As RPost further employs a free-to-use service plan for individuals, with simple add-ins for Gmail and other consumer email offerings, RESPRO® members can not only protect their staff, but also may recommend consumers engaged in the home buying process to install RMail to mitigate consumer risk.

RMail is proven as the simplest to use for both senders and recipients, and provides all of these functions combined in an all-in-one add-in for Microsoft Outlook, Gmail, iPad, for automated sending, and/or in other simple-to-use integrations and web interfaces.

RMail also includes additional features valued by real estate services professionals, such as secure certified file sharing and transfer (to exchange transaction documents that might be too large for email), Digital Seal® sender authentication, and “whaling” attack detection functions (for recipients to authenticate original author of an email, its original content, and its original time of sending).

As a result of this evaluation, RESPRO® has endorsed RPost technologies for cyber security and compliance for use by members and those affiliated businesses operating in regulated industries involving the handling of consumer information.

Due to today’s cyber security risks, heightened regulatory enforcement environment, legal considerations, and need for a simple end-user experience, **RESPRO® recommends members use RMail® services by RPost.**

- ☐ RMail® Registered Email™ service for compliant legal proof of email delivery for TRID (TILA/RESPA Integrated Disclosures) and other notices,
- ☐ RMail® email encryption service with auditable proof of privacy compliance with consumer nonpublic personal information (NPI) privacy rules, and
- ☐ RPost’s RMail®, RSign® or RForms™ e-signature services to electronically record agreement and consumer consent.

RESPRO® entered into a partnership with RPost under which RESPRO® members can subscribe to the RMail service at a discounted rate, as a “one-stop-shop” for compliant email encryption, e-delivery proof, and legal electronic signatures.

Gold Standard Endorsement

Why RMail as the Top Choice for Email Encryption (for NPI Privacy Compliance)

- ☐ RESPRO® knows its members need to demonstrate that they are leaders in terms of protecting consumer rights and information; and that means using secure encrypted email that not only simplifies protecting the privacy of consumer information, but also meets the most stringent compliance requirements.
- ☐ RESPRO® identified RPost as the only secure messaging provider that meets and exceeds member requirements in terms of user simplicity, security, and proof of fact of compliance with data privacy and disclosure e-delivery rules.

- RESPRO® believes members prefer RPost's direct delivery encryption due to its user simplicity, over others' link-retrieval-registration encryption schemas that have been reported to frustrate many users.

Why RMail as the Top Choice for E-Delivery Proof (for TRID and Other Notices)

- RESPRO® knows its members need to focus on keeping the residential real estate transaction process simple and streamlined, while demonstrating that they are leaders in terms of protecting consumer rights and meeting the most stringent TILA/RESPA Integrated Disclosure (TRID) rules.
- RMail e-delivery proof services are built upon RPost's patented Registered Email™ technology, which returns Registered Receipt™ e-delivery proof records that can be authenticated and serve as court-admissible proof-of-compliance records.
- The RMail® Registered Receipt™ e-delivery record:
    - Returns the most robust delivery audit trail which is cryptographically associated with the message content packaged as a self-contained electronic record that is **durable, verifiable, and portable**.
    - Authenticates on-demand by any sender or any expert, and can be easily shared with any challenging party while maintaining the ability to authenticate delivery, timestamps, and content. The authentication process is as simple as forwarding the Registered Receipt by email.
    - Withstands challenge as it has been successfully used as delivery proof evidence in state and federal courts.
    - Approved by lenders as a record worthy of reliance to prove TRID compliance sufficient to substantiate loan transfers.

Why RMail As the Top Choice for Legal E-Signatures (to Record Consumer Consent)

- RESPRO® knows many of its members use e-signatures in parts of their business. RESPRO® believes that having one uniform record serve as auditable proof (of privacy, e-delivery, and e-signature compliance) is a benefit. RPost provides this, and has market-leading e-signature service features and user experiences built into

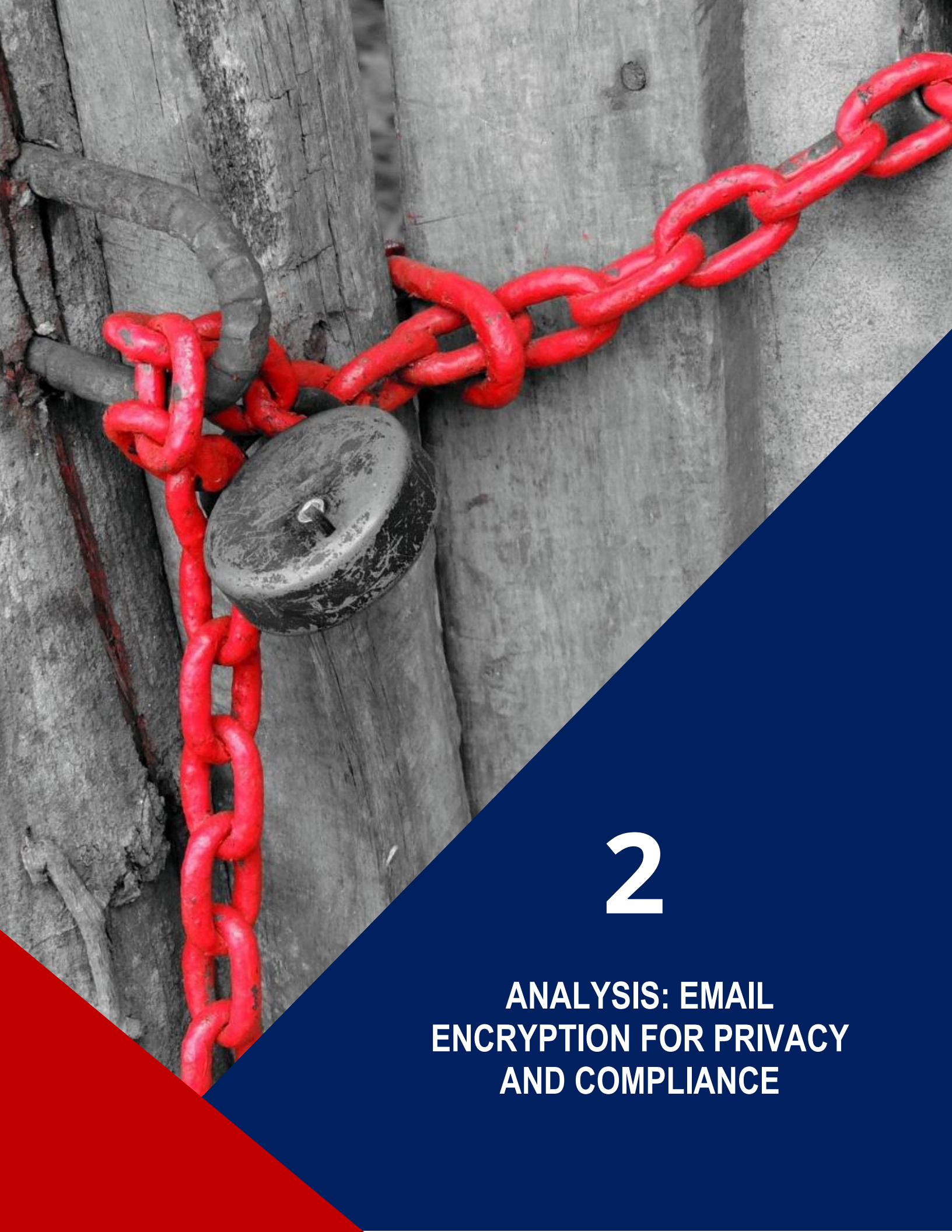
its RMail service, with advanced options in dedicated e-signature and digital forms platforms.

- ☐ RPost received top scores by Forrester Research, Inc., a leading technology analyst, in the areas that RESPRO® identified as most important to member needs:
  - Compliance with ESIGN and UETA laws (5 out of 5)
  - Breadth and depth of e-signature services in terms of features and related services (5 out of 5)
  - Simplicity of user experience in terms of sending and e-signature capture (4 out of 5)
  - Enterprise scalability (5 out of 5)
  - Robust e-signature strategy to continuously improve offerings (4 out of 5)
  - RPost was rated in this Forrester Research report[1] as among the top five e-signature providers overall.
- ☐ As RPost's e-signature technologies are included within its RMail® offering, there is a significant benefit to using RPost® to simplify supplier management and to maintain one uniform compliance record that has high evidential weight -- the Registered Receipt™ record.
- ☐ RPost's RMail® Registered Receipt™ record is a robust and court admissible[2] record of ESIGN and UETA[3] compliance.
- ☐ RPost e-signature services have been vetted and approved by leading investors as ESIGN compliant (financial institutions that are usual purchasers of real estate loans).
- ☐ RPost also offers specialized e-signature platforms: RSign® for web based e-signatures and templates, and RForms™ for PDF forms automation.

Member discounts available at **www.rpost.com/respro**

---

[1] Forrester Research, Inc. The Forrester Wave™: E-Signatures, Q2 2013. Categories paraphrased to match RESPRO® criteria of importance.
[2] Locke Lord Bissell & Liddell LLP Legal Review of RPost Registered E-mail service in context of Electronic Law relative to Authentication / Admissibility Requirements. Abstract.
[3] UETA means Uniform Electronic Transactions Act. ESIGN means Electronic Signatures in Global and National Commerce Act.



2

ANALYSIS: EMAIL ENCRYPTION FOR PRIVACY AND COMPLIANCE

II. ANALYSIS: EMAIL ENCRYPTION FOR PRIVACY AND COMPLIANCE

RESPRO® evaluated several email encryption solutions based on members' feedback, analysts' recommendations and RESPRO®'s own internal assessment.

Email Encryption Solutions Evaluated:

The following services were evaluated:

- **RPost - RMail Email Encryption:** direct encrypted delivery to recipient's desktop, without web login required for recipient or sender, coupled with auditable proof of compliance for every message sent. There are a variety of configurations for sender and recipients, and for automation.
- **Cisco - Email Security Appliance:** on premise appliance that relies on web-based encryption keys to encrypt and decrypt emails, with a recipient link-retrieval-registration process.
- **Axway - MailGate SC:** appliance based platform (with virtual appliance and cloud options) with encrypted files stored on internal servers, with a recipient link-retrieval-registration process.
- **Zixcorp - ZixMail:** store and forward cloud-based encryption, where recipients that have not also signed up and installed software with TLS enabled need to register and login to Zixcorp website to access the message.
- **Hewlett Packard - HPE Voltage:** combination of on-premises and in the cloud deployments, with web-based encryption key management, and encrypted files stored on internal servers, with a recipient link-retrieval-registration process.

Note: There are other email encryption technologies such as PKI (public key infrastructure) certificates and PGP (pretty good privacy) keys that require key exchanges. These are not evaluated here as they are not practical solutions for RESPRO® members due to the complexity of the user experience for sender and receiver, key exchange requirements, and often compatibility requirements with email programs. There are also companies that private label third party solutions or offer their own new solutions; most of these offering a store-and-forward link-retrieval recipient registration process similar to the Zixcorp example noted above, or an HTML file wrapper system similar to the HPE Voltage example noted above.

Evaluation Criteria:

The solutions were evaluated in three areas:

1. Compliance and Security Intelligence
2. Simple User Experience
3. Breadth of Offering with Required Features

1. Compliance and Security Intelligence

As all providers evaluated satisfy the minimum encryption algorithms required by regulations and federal government standards, the key purchase driver is no longer whether or not the encryption solution is 'secure enough' but is how well the solution will protect from fines, lawsuits, and most important of all, loss of reputation.

Auditable proof of compliance with data privacy rules, therefore, becomes a critical requirement of an encryption solution when the use of such solution is required by law, and when it becomes vital to prove, in case of a data breach, that a particular communication was sent and delivered in a compliant encrypted manner to each intended recipient. In 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 may need to prove that the breach did not happen "on their watch".

A data breach can occur in these two scenarios:

- ☐ When the data is within the sender's control (i.e. where the email is sent from sender to recipient - "*security of sender-controlled data*"); and
- ☐ 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 (covered in the next section, *Simple User Experience*).

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*.

The important concept to consider is not which service is more secure (assuming they all meet the security baseline); but how well they protect from fines in a compliance audit, legal, or regulatory examination after a reported breach of private information or breach of TRID document delivery and receipt rules.

The following are commonly used as a record of compliance in the case of a data breach or examination; but these methods often fall short, considering:

- *Text server logs:* It can be difficult, expensive, or impossible to often (a) find these logs, especially if the message was delivered by an email sender or email provider outside of your realm, (b) irrefutably associate the logs with specific message content and timestamps, (c) prove the text files are authentic when authenticity is challenged, and finally, (d) prove that the transmission was sent and successfully received, encrypted.
- *Sent item records:* These will often show the content originated in your organization, but will not demonstrate that the message was transmitted, whether successfully received, and when, or whether it was sent and received encrypted. Often email encryption providers will push messages out circumventing the normal outbound email flow using HTTPS connections, which further complicates sent item tracing.
- *Archive services:* These often tout logging all items sent out, and separately, items 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 its intended recipient; rather, they are logging that a message (often without any easy method to associate message content) has been sent and separately, they log other inbound messages received. Consequently, an archive service typically is not able to identify if a particular message in question has been sent AND received by its intended recipients, and whether it was sent AND received encrypted. Generally, archives will record less than half of the activity – that the message claimed to have been sent, reached the sending mail server prepared for sending.

In contrast, auditable proof of compliance consists of a robust audit trail of delivery that can be independently verified as to fact of encrypted delivery, message content associated

with the delivery record, and uniform timestamps of sending and legal receipt. This record should be durable (meaning, it can be forwarded and retains its ability to be authenticated), verifiable, and self-contained (meaning, all the data to prove delivery, content of the message and attachments, timestamps, forensic records, and fact of encrypted transmission are embedded within the record itself and mathematically associated).

In terms of reporting, the solution should include automated reporting back to the sender organization, so there is adequate visibility into how the services are being used, whether they are being used, and who is or is not using them. Robust reporting is critical to identifying training gaps (and adjusting accordingly), evaluating whether usage patterns by certain users are appropriate, and testing the effectiveness of policies.

Another aspect that is important to consider is the access to the data (for discovery needs, for example), after it was sent in an encrypted manner. Often, when documents are uploaded to a web-based solution for transmission of a download link to the recipient, that document will likely not be stored in a manner that can be easily retrieved as a transmission record, as the upload would have bypassed the normal email server, messaging archive and/or outbound SMTP email compliance tools (bypassing by way of an HTTPS connection). And if the message is encrypted at the mail gateway, some organizations may be concerned with unencrypted transmission within the sender's organization, which may leave a vulnerability in terms of access to protected data. Further, in terms of electronic discovery needs, although the archive may retain a record of what was sent, it will not prove what was delivered or provide uniform timestamps to confirm time of receipt, nor will it prove fact of encrypted delivery to the intended recipient – and most likely, also will not prove e-delivery of disclosures sufficient to transfer loans.

Finally, we also evaluated how well each solution provided tracking and visibility on sent messages. When sending email encrypted, the sender needs to have confidence that the message was transmitted encrypted, and the recipient needs to know that the message received was transmitted encrypted. What if a content-filtering mechanism is not working properly? Senders with most appliances/filters may have no way of knowing immediately when the filter stops working properly, and each day of improper function may cause escalating risk of fines associated with data breach regulations. On the recipient side, a recipient needs to be 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. However, when using TLS to transmit a message encrypted, the message received looks just like a normal email. This lack of awareness by the recipient creates the potential for inadvertent forwarding or other misuse of the protected information.

2. User Experience

Ease of use by sender & recipient means more use and less exposure. The secure encrypted email dilemma is how to deliver the message securely without negating key benefits of email – simplicity and ubiquity – so it is simple enough that it is used in practice, yet secure enough to protect and comply.

There is often a tradeoff between security and simplicity – and often "simplicity" loses the battle, until a company learns that its "secure system" is not actually being used (due to an overly complex user experience). More secure, but too cumbersome, means less used and potentially more exposure.

Data and visibility into use patterns, policy effectiveness, elegant and simple user interfaces, 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 embraced by users and all sensitive messages are sent encrypted.

Encryption services generally have one of two different delivery models:

- **Encrypted Delivery Direct**: The recipient receives the encrypted data right in their inbox and the recipient does not have any requirements to be online to decrypt or view the message. There is no storage of message content by third party service providers.
- **Store-and-Forward Link Retrieval**: Third-party systems store the message content and/or the encryption key in an online repository. The recipient must register and arrange for a password exchange, and the recipient must be online to retrieve and download the message. The sender often does not have a sent email record or record of delivery of the notice to the recipient, instructing him or her to retrieve, register, and download. Some of these systems store the encryption key online and the encrypted message content is sent to the recipient, then back to the system for decryption, and is finally displayed for download in a web browser.

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, and then downloading the message to their desktop. These solutions have lower response rate for clicking through to download the material. Some of these store-and-forward systems require recipient registration for authentication; however, if there are hurdles to getting the information to the recipient, the fallback is unfortunately for the sender to re-send the email unencrypted.

When considering simplicity for recipient workflow addresses (in the case that a generic destination address such as *request@titleinsuranceco.com* is accessed by many individuals), the solution should have mechanisms to deliver to those workflow addresses in a way that multiple recipients with access to the mailbox can decrypt the messages.

Sending automation is also a consideration when considering user simplicity. Sending automation is important when there is a need to filter messages by policy and auto routing for encryption, and to send large batches of encrypted emails.

3. Breadth of Offering with Required Features

With increasing user requirements to not only comply with privacy and consumer protection laws, but to also become more productive and efficient, we considered what other features are offered with the encryption solution in terms of sending apps, encryption features, additional (non-encryption) features, and configuration flexibility.

- *Sender Apps:* Different methods of integrating email encryption services into existing email offerings, embedded within sender email applications such as Microsoft Outlook, Gmail, Salesforce.com, and mobile devices.
- *Encryption Features:* When sending a message encrypted, there are other features that should complement the offering to meet the needs of the real estate industry, such as encrypted reply (even if the recipient is not a subscriber), easy attachment of files of any format, secure file transfer (for files that exceed typical email limitations), and an encrypted e-signature process.
- *Breadth of Related Offerings:* With renewed interest in certified e-delivery proof and timestamps, and electronic signature execution, it is important to consider solutions that combine, on a message-by-message basis, compliant encryption with other services such as electronic contract execution, certified e-delivery proof, and secure large file transfer.
- *Encryption Configuration Flexibility:* There should be 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. The three most common encryption modes are:

    a) Encrypt the message locally at the sender's desktop or mobile device, ensuring encrypted delivery straight through to the recipient's desktop.

b) Encrypt the message at least from the edge of the sender's network to at least the edge of the recipient's network.
c) Encrypt messages at the sender's outbound mail gateway based on message content or other criteria, to the recipient's mail gateway or desktop

4. Weighting Top Level Criteria

RESPRO® considered the importance of each of the top level criteria in today's business environment, and weighted these in order of importance to provide more emphasis on the most important criterial – Compliance and Security Intelligence. Second was "Simple User Experience" and third, "Breadth of Offering with Required Features".

Email Encryption – Solution Scorecard:

Based on RESPRO®'s testing, member interviews, and analysis of its reference email encryption vendors on the three top level purchase drivers described here, the resulting scorecard for email encryption follows, with RPost's RMail® Email Encryption service receiving top scores in each category and overall.

RPost scored noticeably higher than the closest comparable. For this reason, RESPRO® endorsed RPost's RMail Email Encryption for member use.

Table: Email Encryption Solution Scorecard

			Solution Scorecard *(3 is high, 1 is low)*				
Rank	***Top-Level Purchase Drivers***	*Weight*	**RMail**	**Cisco Email Security Appliance**	**Axway MailGate SC**	**ZixCorp**	**HPE Voltage**
1	**Compliance & Security Intelligence**	*1.5*	**11**	**4**	**5**	**4**	**1**
	Auditable Proof of Compliance		*3*	*0*	*0*	*0*	*0*
	Reporting		*3*	*1*	*1*	*1*	*0*
	Electronic Discovery and Data Access		*2*	*1*	*2*	*1*	*1*
	Tracking and Visibility		*3*	*2*	*2*	*2*	*0*
2	**User Experience**	*1*	**11**	**9**	**6**	**6**	**7**
	Sender User Experience		*3*	*2*	*1*	*1*	*2*
	Recipient User Experience		*3*	*2*	*1*	*1*	*1*
	Recipient Workflow Addresses		*2*	*2*	*2*	*2*	*2*
	Sending Automation		*3*	*3*	*2*	*2*	*2*
3	**Breadth of Offering & Features**	*0.5*	**12**	**8**	**8**	**6**	**6**
	Variety of Integrated Sender Apps		*3*	*1*	*1*	*1*	*1*
	Feature Requirements		*3*	*3*	*3*	*2*	*2*
	Breadth of Related Offerings		*3*	*1*	*1*	*0*	*0*
	Configuration Flexibility		*3*	*3*	*3*	*3*	*3*
Total	**Scores with Importance Weighting**		**34**	**19**	**18**	**15**	**12**

3

ANALYSIS: ELECTRONIC DOCUMENT DELIVERY FOR TRID COMPLIANCE

III. ANALYSIS: ELECTRONIC DOCUMENT DELIVERY FOR TRID COMPLIANCE

Driven by the new CFPB requirements, lenders and brokers are increasingly moving to e-delivery of disclosures to realize several benefits:

- ☐ Record the customer's intent to proceed (prior to collecting the processing fee),
- ☐ Move the disclosure process to electronic, with proof of digital delivery,
- ☐ Rely on audit trails to demonstrate compliance in case of audits, and
- ☐ Shorten the closing timeline.

While the CFPB does not specify how to prove sending or delivery, RESPRO® recommends that if doing so electronically, members should use a service that provides auditable proof of e-delivery sufficient to support a challenge in a compliance audit, examination, and importantly, to provide confidence of compliance sufficient to transfer the loan.

In the context of e-delivery proof, auditable proof of compliance consists of a robust audit trail of delivery that can be independently verified as to fact of sending and delivery as defined by the Uniform Electronic Transactions Act Section 15, message content associated with the delivery record, and uniform timestamps of sending and legal receipt. This record should be durable (meaning, it can be forwarded and retains its ability to be authenticated), independently verifiable (meaning, any party that holds the record can verify the authenticity of the record content), and self-contained (meaning, all the data to prove delivery, content of the message and attachments, timestamps, and forensic records, are embedded within the record itself and mathematically associated).

The greatest risk of not using a service that maintains a sufficient record may be the risk that the RESPRO® member must hold the loan principal, caused by inability to prove disclosure compliance sufficient to transfer the loan.

For all members, considering today's heightened regulatory enforcement environment, "good enough" may not be acceptable. RESPRO® advises use of the best – to demonstrate to the market members' interest in protecting consumer rights.

E-Delivery Solutions Evaluated:

The following solutions were evaluated:

- ☐ **Registered Email technology:** email add-on service that certifies delivery and content, and generates a durable, verifiable, and self-contained electronic receipt for every transaction.
- ☐ **SMTP Relay:** routes email through a third party to deliver high volumes of emails.

- **SMTP + Link:** relayed email through a third party, with an image stored in the third party server, downloadable through a link.
- **File Sharing:** files are uploaded to a third party server, and recipient receives an email with a link to access the file, or is granted access to a folder to upload and/or exchange files.
- **Sent Archive:** electronically stored copies of email sent in an archive.

Evaluation Criteria:

The solutions were evaluated on the same criteria we used to compare the email encryption solutions:

1. Compliance and Auditable Proof
2. Simple User Experience
3. Breadth of Offering & Features

1. Compliance & Auditable Proof

When evaluating the potential issues of electronic delivery of 3-day notices and other required disclosure and closing documents, as well as other important communications, there are four potential costs that stand out:

- Claims of non-receipt by the receiving party
- Disputes around time of receipt and disclosure compliance
- Challenges to content of message disclosure
- Inability to transfer loan due to lack of compliance proof

While some may consider the standard for TRID e-delivery to be a record of the precise content that was legally sent, RESPRO® advises members to also retain a record that demonstrates irrefutable legal delivery. This record must be capable of supporting a compliance audit or claim of insufficient disclosure in a legal action.

For some members, the cost of not maintaining records of e-delivery proof may be the cost of having funds tied up holding a loan for the duration, without the ability to sell it. For others, it may be continued inefficiency or lost deals due to delays that result in cancellations due to extra time to close, providing a greater window for interference from buyer's remorse or competitive bidding.

How might one prove fact of sufficient e-delivery of a disclosure?

- Firstly, consider what information should be disclosed. What is considered important for audit or compliance proof is the ability to irrefutably demonstrate the precise content that was disclosed.
- Secondly, to prove that the disclosure was clear, one should be able to re-construct the original disclosure in form and format, to demonstrate how the information was originally displayed.
- Thirdly, to demonstrate that the disclosure was accessible to the recipient, it may be important to be able to show how the information was delivered to the intended recipient. For example, if the disclosure was attached to an email in a standard PDF or inserted as body text in the email, and delivered to the recipient's inbox, this would mean the information was accessible.
- Fourthly, the record that is relied on as proof of the above – the original content, the content inside its original context, and accessibility of the content to the intended recipient -- should be in a form that is verifiable, durable, self-contained, court-admissible, and timestamped.

The Uniform Electronic Transactions Act (UETA) provides a useful definition of what constitutes the time of a '*legally received electronic message'* within UETA (sections 15(b) and (e)):

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 retrieves the email), when it enters the recipient's "information processing system" or server that the recipient uses to receive email.

RESPRO® evaluated solutions on how or whether they included the following audit elements that would give a strong evidentiary record to a sender of an electronic communication, should a recipient later challenge receipt of a disclosure document[4]:

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 associate and preserve as tamper-detectable the contents of email and their attachments so as to satisfy process requirements designed under UETA, and the Electronic Signatures in Global and National Commerce Act (ESIGN);

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 ESIGN and UETA, the recipient of the electronic transmission must have consented to the use of electronic format as opposed to paper, use of e-signatures, and to receive notices at a particular email address; with a record of the recipient's consent retained as a reproducible legal record to prove consent if challenged.

With regards to tracking and visibility, the SMTP relay solutions provide only some levels of delivery tracking if recipient systems are set to return notices of delivery failure and if these are properly cataloged and associated with sent messages. Most relay systems have limitations.

Some SMTP relay systems store an image at a link to track email opening if the link calls to the server to deliver the image. However, these only provide information to the sender

[4] Locke Lord Bissell & Liddell LLP Legal Review of RPost Registered E-mail service in context of Electronic Law relative to Authentication / Admissibility Requirements. Abstract. Available at www.rmail.com.

about opening if the recipient sets their system to display images and return that information back to the originating system. For example, recipients reading email using Microsoft Outlook with default settings have an email program that does not display these images to trigger the return of the open/delivery information. Further, the sender would need a verifiable means to associate the content of a particular message with the record of opening; and typically these open records are presented in simple text that can be easily altered, or in web views that are difficult to use when one needs to transmit the record to parties as proof, since the information is often not self-contained, to include delivery timestamps and content record with a verification process.

Considering the UETA legal definitions of what is deemed the 'time of sending or receipt' of email, it is not at all practical to rely on these SMTP relay or SMTP + link tracking systems for proof of compliance with delivery 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 easily be able to prove that that the notice has been 'legally' received.

While file sharing services provide some information about delivery if the recipient takes compliant action and collects the document by visiting the file sharing website to download the file, these don't provide information in a manner that would have significant evidentiary weight as there is limited verification of delivery and content, and the verification is dependent on action by the recipient. Similarly, e-sign services used to deliver documents often require recipient actions.

2. User Experience

Sender experiences for the e-delivery alternatives evaluated differ in that some require processes to manually upload files, or programming to automate sending using application programming interfaces. Use of outbound email is preferred, in particular if one can automate sending from business applications without the complexity of programming, and one can send from common email programs such as Microsoft Outlook and Gmail – all the while having one uniform record regardless of the sending method or platform, or whether the information is sent automated or by an individual.

1. The recipient experience also varies substantially based on the e-delivery alternatives considered:

    a) **File Sharing / SMTP with Link**: These solutions require the sender to upload or send the file 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. There are two challenges with using store-and-forward file transfer services as a method to prove e-delivery:

b) *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 downloadable documents or read the 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 entire email content from the sender.

c) *Inability to prove notice reception:* Since a standard email is generally transmitted from the store-and-forward system to the recipient, requesting that the recipient 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).

- **Direct Delivery**: The recipient receives the email and attachment data right in their inbox and the recipient does not have any requirements to be online to view the message. There is no third party storage of message content. There are no special compliant actions required at the recipient side.

Workflow management and e-delivery automation of closing and related documents are desirable features, which can be more easily achieved with systems that offer email sending integration versus uploading of documents and files.

3. Breadth of Offering with Required Features

Evaluating what other features are currently available or can be offered with the selected e-delivery solutions provides additional comparison viewpoints:

- *Sender Apps:* Sending from common email clients such as Microsoft Outlook, Gmail, Salesforce.com, from real estate and title management platforms, and from mobile and tablet devices.

- *E-sign*: options to record consent.
- *E-delivery Features:* Such as file format compatibility, file transfer for large files, e-delivery records and audit trail.
- *Breadth of Related Offerings:* Such as electronic signatures and encryption.
- *E-delivery Configuration Flexibility:* Out-of-the-Box configurations and availability of custom settings for enterprise needs and automation.

4. Weighting Top Level Criteria

RESPRO® considered the importance of each of the top level criteria in today's business environment, and weighted these in order of importance to provide more emphasis on the most important criterion – Compliance and Auditable Proof. Second was "Simple User Experience" and third, "Breadth of Offering with Required Features".

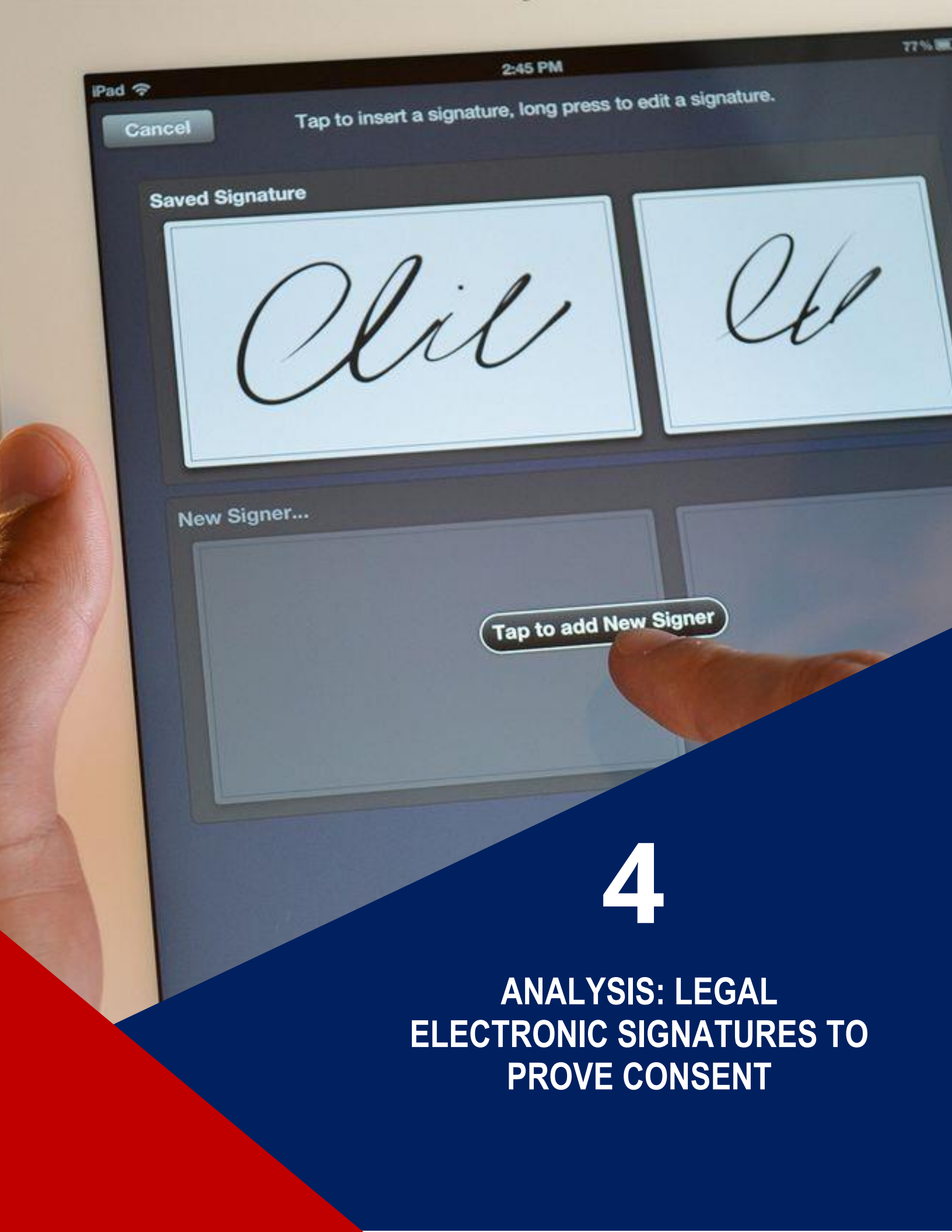
E-Delivery Proof – Solution Scorecard:

Based on RESPRO®'s testing and analysis of its reference e-delivery alternatives in the three top level purchase drivers, the following is the resulting scorecard for e-delivery proof.

RPost's RMail® Registered Email™ track and prove service not only scored the highest, but it also scored significantly higher than the closest comparable. For this reason, RESPRO® endorsed RPost's RMail® Registered Email™ track and prove service for member use.

Table: E-Delivery Proof Solution Scorecard

			Solution Scorecard *(3 is high, 1 is low)*				
Rank	***Top-Level Purchase Drivers***	*Weight*	**RMail**	**SMTP Relay**	**SMTP + Link**	**File Share**	**Sent Archive**
1	**Compliance & Auditable Proof**	*1.5*	**15**	**3**	**5**	**3**	**2**
	Delivery audit trail record		*3*	*2*	*2*	*0*	*1*
	Open tracking optimization, multiple		*3*	*0*	*2*	*1*	*0*
	Uniform & independent timestamp		*3*	*0*	*0*	*1*	*0*
	Content, time authentication & association		*3*	*1*	*1*	*1*	*1*
	Portability, durability, reconstruction		*3*	*0*	*0*	*0*	*0*
2	**User Experience**	*1*	**12**	**9**	**7**	**4**	**8**
	Sender User Experience		*3*	*1*	*0*	*1*	*2*
	Recipient User Experience		*3*	*2*	*1*	*1*	*2*
	Recipient Workflow Addresses		*3*	*3*	*3*	*1*	*2*
	Sending Automation		*3*	*3*	*3*	*1*	*2*
3	**Breadth of Offering & Features**	*0.5*	**12**	**3**	**4**	**2**	**1**
	Variety of Integrated Sender Apps		*3*	*0*	*1*	*1*	*1*
	Feature Requirements		*3*	*2*	*2*	*0*	*0*
	Breadth of Related Offerings		*3*	*0*	*0*	*0*	*0*
	Configuration Flexibility		*3*	*1*	*1*	*1*	*0*
Total	**Scores with Importance Weighting**		**41**	**15**	**17**	**10**	**12**



4

ANALYSIS: LEGAL ELECTRONIC SIGNATURES TO PROVE CONSENT

IV. ANALYSIS: LEGAL ELECTRONIC SIGNATURES TO PROVE CONSENT

Within the integrated real estate services market, member companies and affiliates have identified significant productivity benefits in use of e-signatures. A primary requirement is to record instant electronic execution of documents and forms in compliance with ESIGN, UETA, and consent disclosure rules.

Investor Criteria

In reviewing investor (financial institution members that are primary purchasers of residential real estate loans) criteria, five principles stand out as most important:

1. Consumer e-signing has become simpler and more accessible, however, companies dealing in highly regulated residential real estate have different needs; they need to control the e-signature process for uniformity of records and confidence in legalities.
2. The electronic signature service providers servicing this industry must provide simple-to-use services that record e-signatures and consent in an ESIGN compliant manner.
3. Often there are requests for customized offerings to automate workflow and records routing. Suppliers must be able to satisfy customizations and feature requests “off-the-shelf”.
4. There is value in one underlying record type for proof of compliance (with e-delivery rules, encryption needs, and e-signoff). There is benefit in one supplier for uniformity of records.
5. Investors (financial institution and funds that are potential purchasers of loans) must be comfortable in the proof of compliance with recording consent to conduct elements of the transaction using a particular email address.

Some investors set forth processes to approve e-signature suppliers. They generally aim to confirm if the provider operates with:

1. Strong authentication and authorization,
2. Comprehensive logging, monitoring, verifiable forensic audit trails, mathematical content and timestamp association,
3. Use of encryption, data integrity verification, access controls,

4. Simple and intuitive user experience, with workflow automation rules and templates,
5. Industry standard operations processes for change control and security.

The result of the e-signature process is to obtain a returned ESIGN and UETA compliant record that can be verified. In terms of ESIGN compliance, one looks to confirm consumer consent to conduct the transaction using a particular email address, in electronic format, and with use of electronic signatures. Consent with UETA regulations additionally center on UETA Section 15 in terms of what constitutes the legal time of sending and receiving of an emailed disclosure notice.

In leading systems, a sender receives a visible signature record in PDF format with timestamps and audit trail information. This signature may be authenticated, recording the action, and cryptographically sealed to the transaction audit trail, content, and timestamp information.

RESPRO® Top Level Evaluation Criteria

In terms of e-signature use within RESPRO® members and affiliates in the integrated real estate services market, RESPRO® has identified the following top level evaluation criteria:

1. Compliance with ESIGN and UETA laws
2. Breadth and depth of e-signature services in terms of features and related services
3. Simplicity of user experience in terms of sending and e-signature capture
4. Enterprise scalability
5. Robust e-signature strategy to continuously improve offerings

Forrester Research, a leading technology analyst, identified five companies that lead the e-signature market, considering their review criteria.

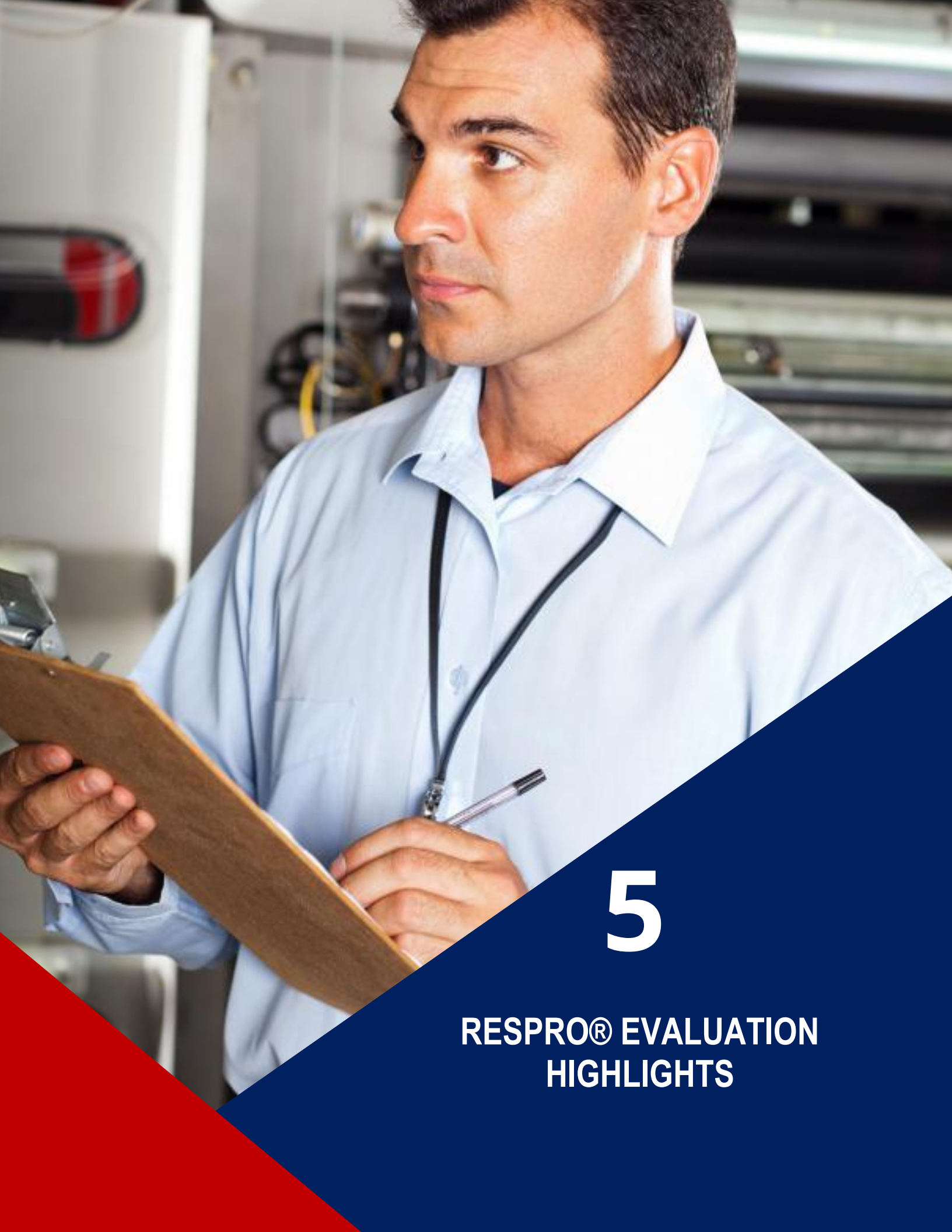
Forrester Research, Inc., in their The Forrester Wave™: E-Signatures report, reviewed e-signatures suppliers considering the following elements: e-signature capture, sender configuration and customization, user experience, mobile platform support, forms and data, global support, compliance with industry/country regulations and technical standards, signature workflow management, integration flexibility, authentication, digital signature, electronic evidence, enterprise scalability, breadth and depth of e-signature services, and e-signature strategy. Forrester Research scored leading e-signature service providers and identified the leaders worldwide.

E-Signature – Criteria Rating:

RESPRO® endorses RPost's e-signature technologies for member use, as RPost received top scores for the criteria RESPRO sees as most important for its members and their affiliates,

a) RPost has been rated among the top five e-signature providers worldwide by Forrester Research in the previously mentioned report, with top scores adding to 23 out of 25 for the above five categories that RESPRO believes are most important to member needs.
b) RPost's e-signature technologies are included within its RMail® offering. There is a significant benefit to using RPost® to simplify supplier management and to maintain one uniform compliance record that has high evidential weight, the Registered Receipt™ record.
c) The RPost's Registered Receipt™ record is likely the most robust the record of ESIGN and UETA compliance. The Registered Receipt email record includes the original message/documents, PDF signoff consent/documents, biometric scripted signature, forensic audit trail, and transaction meta-data, all cryptographically associated to support any third-party authentication request.

RPost e-signature services have been vetted and approved by leading investors (financial institutions that are usual purchasers of real estate loans) as ESIGN compliant. RPost also offers standalone RSign® web based and RForms™ PDF forms automation specialized e-signature platforms.



5

RESPRO® EVALUATION HIGHLIGHTS

V. RESPRO® EVALUATION HIGHLIGHTS

RMail® Encryption (for Security and NPI Compliance)

RPost's RMail encryption service leads in key areas important in regulated industries:

- ☐ **Simplest to use** from both sender and recipient perspective, whether sent by individuals or from automated systems. Simple to use means more users adopting the solution and more compliance.
  - Install in Microsoft Outlook or Gmail; or send from automated applications without software changes.
  - Automatically detects best secure delivery method based on the recipient email environment, considering both security and user simplicity for the recipient.
- ☐ Certified proof of compliance.
  - Returns auditable proof of data privacy compliance.
  - Certifies proof of timestamped content legally delivered to satisfy TILA/RESPA Integrated Disclosure (TRID) rules and other time-dependent notice delivery rules.
- ☐ Comprehensive and feature rich.
  - Includes all of the service functionality required by the most sophisticated enterprise technology departments while maintaining overall user simplicity.
- ☐ **All-in-one secure messaging solution**, with a wide range of services included.
  - The RMail encryption service is part of the all-in-one RMail® service, with certified e-delivery proof, e-signatures, and secure large file transfer.

Compliance & Security Intelligence

Compliance: Compliance requires sending securely, with court admissible proof of fact of encrypted delivery. RMail services return (a) a Registered Receipt™ record using patented technology; and/or (b) a sealed certified report. Both provide auditable proof of e-delivery for TRID and other time-dependent notices, and proof of fact of data privacy compliance, on a message level or system level.

Reporting & Administration: RMail has the most comprehensive tracking, reporting, and administrative options. RMail services provide comprehensive delivery, opening,

timestamped tracking and status reports scheduled or real-time, returned with selectable levels of detail and a variety of formats to be imported into senders' systems or for individuals to review and analyze.

User Experience

Simple for Sender: The RMail service process is the simplest for senders and receivers. From a sender's perspective, RMail runs within the message compose user interface of Microsoft Outlook (all versions) and Gmail, or can be sent automated from applications.

Simple for Recipient: From a recipient's perspective, RMail automatically detects the best secure method of delivery to the recipient, considering detected recipient configurations and the sender's settings, with direct delivery of the email pushed to the recipient's inbox, and with no messages stored in the middle. There are no links to click and no recipient user accounts to create or register for.

Breadth of Offering with Required Features

Secure Messaging Functions: RMail services include all required functions and security, with the main functions of sender one-click sending options, sender automation, recipient secure reply, and certified tracking.

Breadth of Offering: RMail provides value beyond data privacy, as it includes proof of TRID e-delivery and a complete set of e-sign services. RPost offers all of the functionality a company may need for high value messages, including tracking, certified e-delivery proof, encryption for compliance, e-signatures, secure large file transfer, and more.

RMail® Track & Prove Service (TRID and Notice E-Delivery Compliance)

Verifiable, Durable and Portable Record Authentication

The primary purpose of e-delivery tracking and proof services is to protect the sender or their organization after-the-fact with an irrefutable record of who said what to whom, who delivered what to whom, who received what and when, should there be a later question as to what transpired. In regulated industries, with a high level or risk associated with a claim of non-receipt of a disclosure or transaction term, proof-of-delivery is required.

- **Compliance:** Compliance requires sending messages with and without attachments, with court admissible proof of fact of e-delivery. RMail services return (a) a Registered Receipt™ record using patented RPost Registered Email™ technology; and/or (b) a sealed certified report. Both provide auditable proof of e-delivery for TRID and other time-dependent notices, (and proof of fact of data privacy compliance when applicable), on a message level or system level.

- **Reporting & Administration:** RMail has the most comprehensive tracking, reporting, and administrative options. RMail services provide comprehensive delivery, opening, timestamped tracking and status reports scheduled or real-time, returned with selectable levels of detail and a variety of formats to be imported into senders' systems or for individuals to review and analyze.

With proof-of-delivery services, the record is more powerful if it can be easily forwarded by email to a questioning party and yet maintain its ability by that party or any other to verify the transaction record authenticity. This creates a need to ensure the transaction record is:

a. Complete - includes the delivery history, timestamps, original message content, transaction forensic audit trail

b. Durable and portable - it can be forwarded electronically by any user and the complete record maintains its unique association and authentication capabilities

c. Verifiable – can be authenticated with electronic originals reconstructed by any user without a forensic expert.

The RMail service record satisfies these needs to the highest level, with:

- Delivery audit trail record: RMail includes all server-level dialogs for each send attempt at each stage.
- Multiple methods of open tracking optimization: RMail uses multiple methods of delivery and open tracking to enhance delivery record.
- Uniform & independent timestamp: RMail always provides multiple uniform times source with UTC conversions.
- Content, time authentication & association: RMail cryptographically associates content, time, delivery audit trail & open data.
- Portability, durability, reconstruction: RMail record is self-contained, may be forwarded and retains authentication ability.

The RMail® Registered Receipt™ e-delivery record:

- Provides a robust delivery audit trail which is cryptographically associated with the message content packaged as a self-contained electronic record that is durable, verifiable, and portable.

- ☐ Authenticates on-demand by any sender, any expert or shared with any challenging party, simply by forwarding the receipt by email.
- ☐ Has been successfully used as delivery proof evidence in state and federal courts, and has been approved by lenders as record worthy of reliance as a record of TRID compliance to substantiate loan transfers.

RPost® E-Signature Services (Recording Consent and Agreement)

RESPRO considerations included the following:

Electronic signing is becoming simpler, more accessible, and free. Many leading service providers offer free limited service use for individuals.

However, member companies have different needs than simply accepting documents that have been electronically signed by their customers. Member companies need to control the electronic signature process to have uniformity in their signoff records and to ensure their comfort with the robustness (from a legal and evidential weight perspective) of that record.

Further, member companies need to consider that different business processes can be optimized with electronic signature services tailored to that specific process environment – high volume lower value transactions can use one e-signature process suited for this type of document, while lower volume high value documents may merit another e-signature process. Regardless, uniformity in the legal record memorializing what was signed by whom and when, while reducing legal risk, is important.

RESPRO® identified RPost's e-signature services as having simple processes for obtaining the signature as a foundation, control of the e-signature process across a variety of electronic signature scenarios, and the most robust legal and evidential record of all of the signature event transaction metadata, audit trail, with authentication capabilities.

I. RPost E-Signature Foundational Elements

1. **Reduce Legal Risk:** Legally-signed contracts that may be verified to prove the lifecycle of the process
2. **Simplicity:** Simple e-signature process for both the sender and signer with simple integration for sending automated
3. **Operationally-Proven**: Experience serving consumer and business signers for more than three years.
4. **Security**: Experience processing business-sensitive data

5. **Reporting**: Tracking of document delivery, opening, and signoff
6. **Record:** Signoff record that can be authenticated on demand

II. RPost E-Signature Differentiated Elements

1. **Breadth of eSignature Services:** Variety of electronic signature services off-the-shelf, including:
    a) Sender signing from popular desktop and mobile applications including Outlook
    b) Recipient signoff using click to sign for completed documents where a signature is required
    c) Recipient signoff using hand-scripted signature to capture the biometric, mouse-scripted signature
    d) Forms fill, sign, with data extraction where the recipient views and signs the document using any PDF reader
2. Sending Simplicity and Multiple Means of Access:
    a) Outlook: Signing and sending, and/or sending for recipient signoff without advance document preparation
    b) PDF Forms: Preparing forms for signoff processes and automation in native PDF format
    c) Web: Sending for signoff from a web-user interface
    d) Mobile: Permitting signing, and sending for signoff from Apple and Android mobile devices
    e) Routing by SMTP: Sending documents for signoff, automated from business management systems by email
    f) Routing by Web Services: Sending documents for signoff, automated from business management systems
3. Control and Legal Record:
    a) Document Delivery and Signoff: Cryptographically verifiable record of document delivery, failure, opening, signoff

   b) Portability of Record and Audit Trail: Ability to authenticate the signoff event (documents and Internet forensics associated with the signoff) as a stand-alone record, without any requirements of third-party storage
   c) Uniformity: One uniform verifiable receipt of each transaction, regardless of the signoff process
4. Encryption for Data Privacy:
   a) Document Delivery: Options for encrypted document delivery.
   b) Signoff Process: Options for encrypted electronic signature processes
5. Breadth of Related Services
   a) Email and document delivery proof for notices.
   b) Encrypted email and document delivery with proof of encryption for data privacy compliance.

RESPRO® endorses RPost's e-signature technologies for member use, as RPost received top scores for the criteria RESPRO sees as most important for its members and their affiliates.

RPost also offers standalone RSign® web based and RForms™ PDF form automation specialized e-signature platforms.

RESPRO® Endorsement Summary

RMail services offer the convenience, IT simplicity, and cost efficiency of working with one solution provider for three of today's critical security, compliance, and productivity business needs – managing e-delivery proof, email privacy, and recording legal e-signatures.

RESPRO® identified RMail as the only solution that meets and exceeds requirements in terms of user simplicity, security, and proof of fact of compliance with data privacy and disclosure e-delivery rules. RESPRO® endorses use of the RMail service by RESPRO® members as its all-in-one solution for compliant email encryption, e-delivery proof, and e-signatures.

RESPRO® has negotiated member discounts available at http://www.rpost.com/respro

6

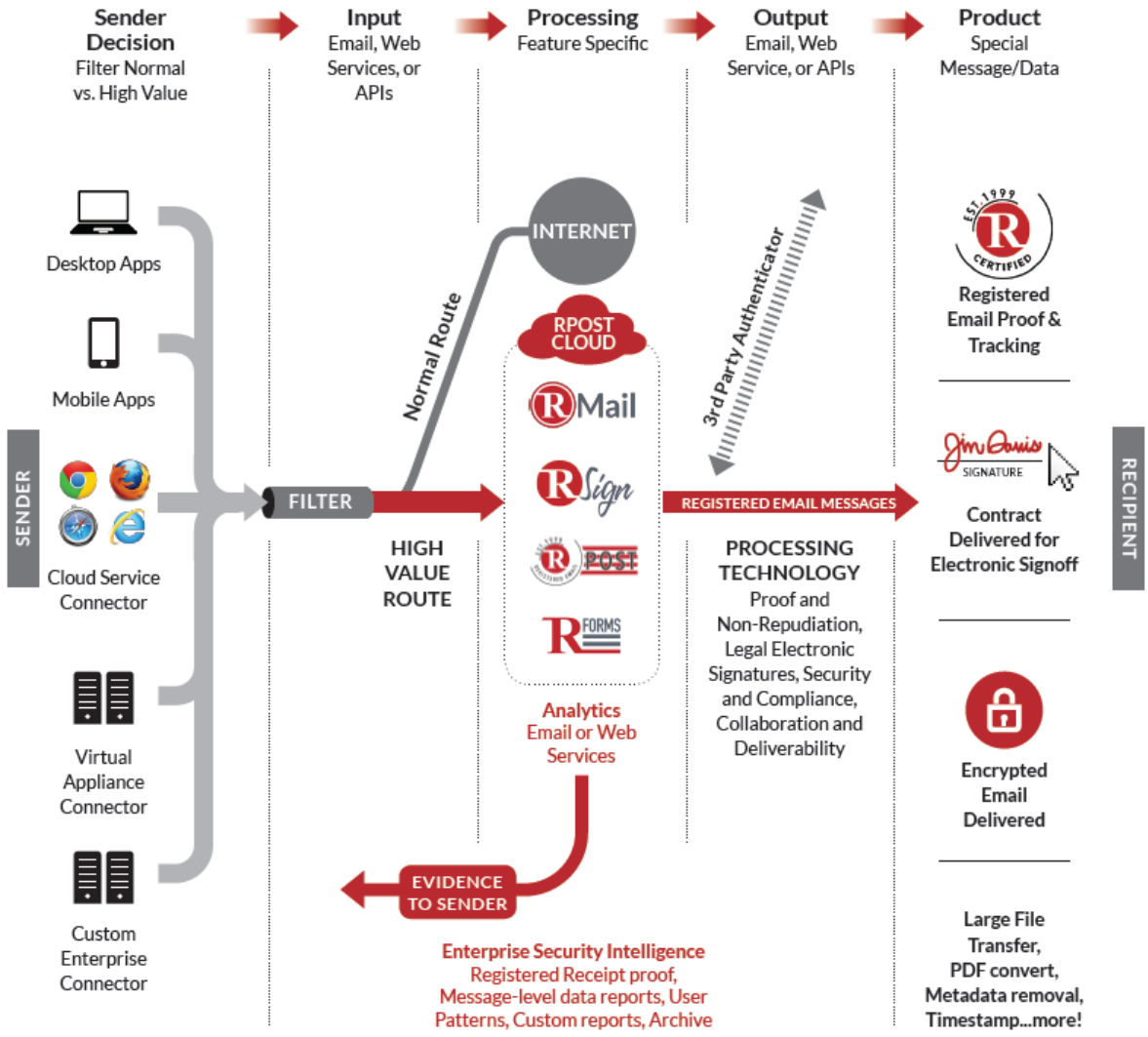
REGISTERED RECEIPT RECORD AS UNIFORM PROOF OF COMPLIANCE

VI. REGISTERED RECEIPT RECORD AS UNIFORM PROOF OF COMPLIANCE

Registered Receipt

A foundational element of the RESPRO® endorsement of RPost services is the Registered Receipt™ email record. This Registered Receipt record is the uniform transaction record returned to the sender for each processed message. It returns the highest evidential level of proof --- verifiable, durable, and auditable proof of compliance with data privacy, e-delivery, and e-signature requirements.

When using the RPost services, the data flows as follows, with the Registered Receipt™ record among the evidence elements returned to the sender.



The Registered Receipt proof is built upon proprietary Registered Email™ technology, with more than 50 patents (listed at www.rpost.com/technologies) that cover tracking electronic

message delivery; authenticating legal time of sending, delivery, and opening; authenticating the content of the message and its attachments; and acting as a third party authenticator of the entire transmission.

The Registered Receipt technology is generally recognized as the standard for certified digital transaction evidence, and maps to published standards and electronic transaction laws, including:

- ☐ Universal Postal Union Postal Registered Electronic Mail standard
- ☐ European Telecommunications Union Registered Electronic Mail standard
- ☐ British Standards Institute 'Legal admissibility' Code of Practice
- ☐ European Electronic Commerce Directive (2000/31/EC)
- ☐ UNCITRAL model law for electronic transactions
- ☐ US Uniform Electronic Transactions Act (UETA)
- ☐ US Electronic Signatures in Global and National Commerce Act (ESIGN)
- ☐ Uniform Commercial Code Article 9
- ☐ Standards and Procedures for Electronic Records and Signatures (SPeRS)
- ☐ US Court Admissibility case law

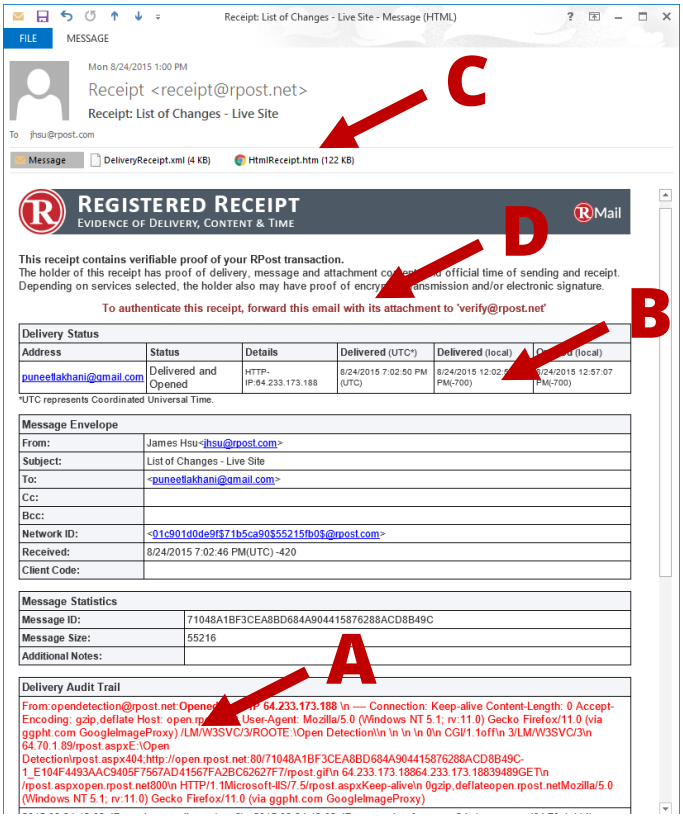
Structure of the Registered Receipt™ Record

The Registered Receipt record is comparable to the record of delivery that a courier or certified receipt mail service may provide. Moreover, rather than simple email tracking, the Receipt provides the sender the means to demonstrate to any party not only that a message was sent, received and precisely when, but also what the message and attachments said (‘who said what to whom and when’), in an easily portable and verifiable form. The Receipt packages the email record so that it has all of the components that would deem it the "best evidence" one would want to submit related to an email record. This will be discussed in the following section.

Legal Proof of Delivery

What is legal delivery?

The Uniform Electronic Transactions Act (UETA) Section 15 provides that an electronic record is considered received by the intended recipient when it enters an information processing system that the recipient has designated or uses for the purpose of receiving electronic records of the type sent and from which the recipient is able to retrieve the electronic record, and is in a form capable of being processed by that system.



In the case of email, this provision means that an electronic message is delivered once delivered to the email server authorized to receive mail for the recipient's address. This might be a recipient corporate mail server or the server of the Internet Service Provider that manages the individual recipient's mail account.

A. Transaction meta-data

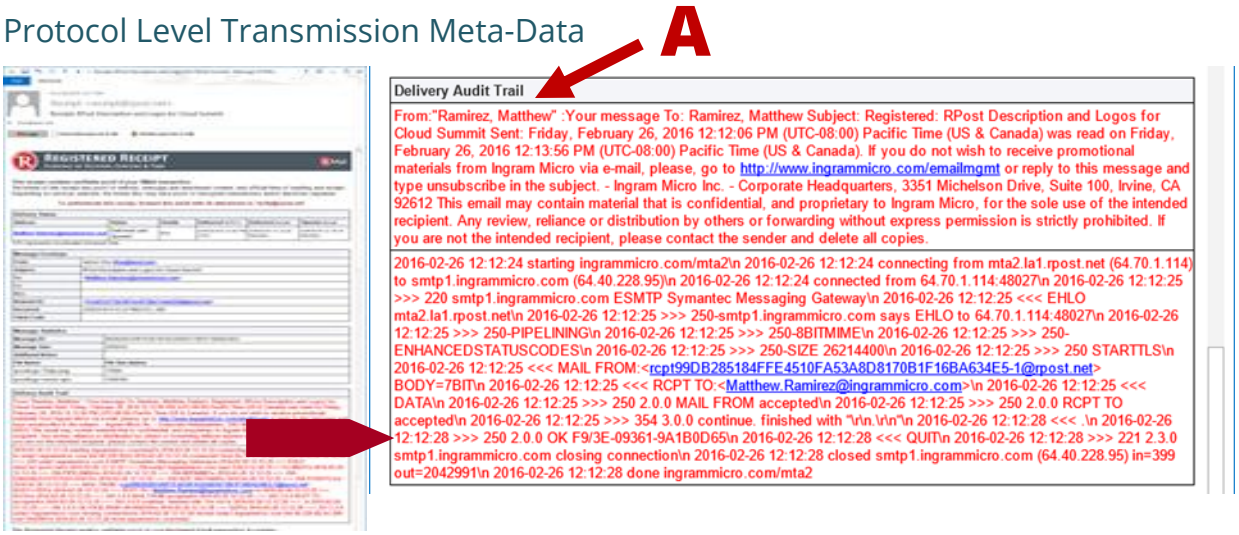
B. Delivery Status for each Recipient

C. Self contained – RPost stores no data

D. Authentication process

The patented technology proves delivery by recording the transactions between the RPost Cloud server and the recipient's mail server as each message is delivered. These transactions are a dialog conducted in the Simple Mail Transport Protocol (SMTP) that governs all Internet email communications. This protocol requires the recipient mail server to: identify itself, declare itself prepared to accept mail on behalf of a named recipient, and acknowledge when the mail has been successfully received. By recording the SMTP dialog (along with other internet forensics), the Registered Receipt email documents the recipient mail server's declaration of accepting the mail, or "signature of acceptance from the recipient's mail room." For each delivered message, a transcript of the dialog is included in each Receipt in addition to other information comprising an audit trail of the message's delivery. Since all Internet mail is delivered via SMTP, the Receipt can provide proof of delivery to any Internet destination.

Protocol Level Transmission Meta-Data



The baseline for legal delivery is “delivered to mail server” or “failure” of the recipient’s mail server to accept that email on behalf of that recipient. Like a courier, the RPost system will work to document the highest level of delivery possible within a period of time - - delivered to mail server (mail room), delivered to mail box (recipient’s desktop), or opened (recipient).

A delivery “failure” can occur for a number of reasons and it is important that the sender know whether or not there was a “failure”, as the sender cannot safely make the assumption that if they do not get a failure notice (bounce notice) with standard email, then their email was received. In fact, many mail server administrators have turned off these “delivery status notifications” as email marketers often use these to determine live addresses versus inactive accounts. A delivery “failure” can result from the message being too large, losing data packets during transmission, not having an address recognized by that recipient mail server, or other reasons such as a problem with the sender’s or recipient’s mail server.

In summary, the four levels of delivery, three being considered ‘legally received’ as defined by the electronic transactions laws and case law, are:

Delivered: Confirmed Opened

Delivered: Minimum Delivery to Mailbox

Delivered: Minimum Delivery to Mail Server

Delivery Failure

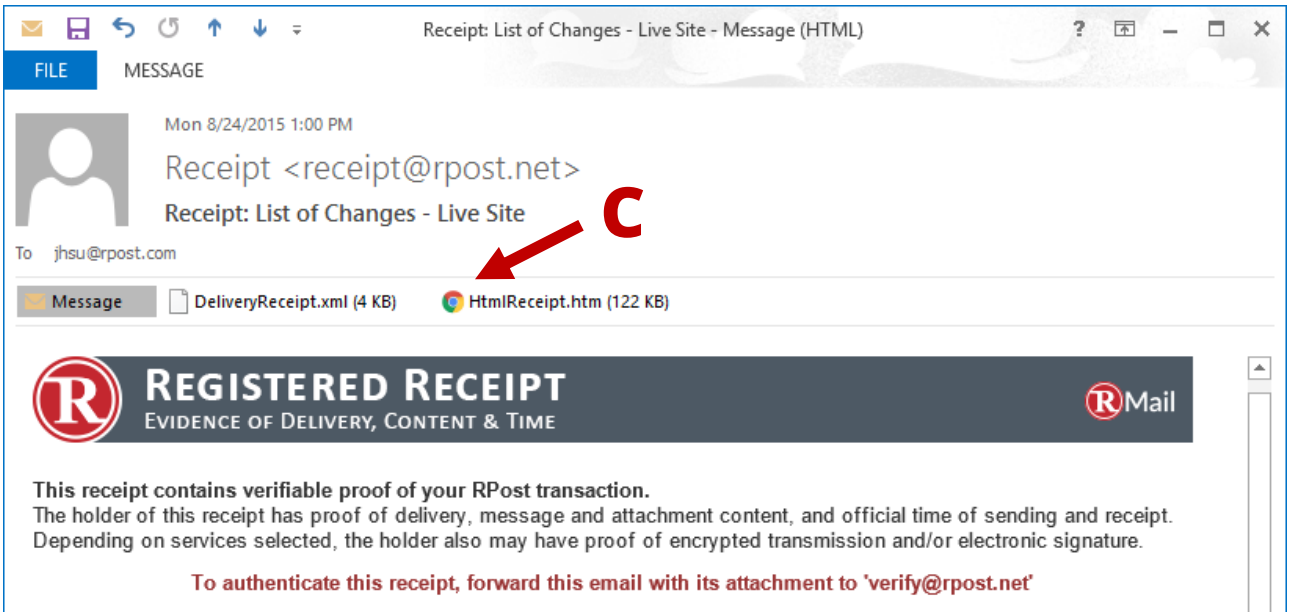
These are analogous to traditional courier and receipt mail service records as noted below.

Registered Email		Traditional Mail Carrier Analogy
☑ Opened	=	Recipient signature
☑ Mailbox	=	Assistant signature, put on desk
☑ Mail Server	=	Mail room attendant signature
☒ Failure	=	No one signs for it

Delivery Status

Address	Status	Details	Delivered (UTC*)	Delivered (local)	Opened (local)
ndavis@rcn.com	Delivered and Opened	Relayed to mailbox mx1.emailsrvr.com (173.203.2.36)	6/11/2014 12:37:25 AM (UTC)	6/10/2014 5:37:25 PM(-700)	6/10/2014 9:58:49 PM(-700)
gmills@ampnetworks.com	Delivery Failed	Returned unopened by mailserver	***	***	
jbroderick@gmail.com	Delivered to MailBox	Relayed to mailbox gmail-smtp-in.l.google.COM (74.125.129.27)	6/11/2014 12:37:26 AM (UTC)	6/10/2014 5:37:26 PM(-700)	

*UTC represents Coordinated Universal Time.



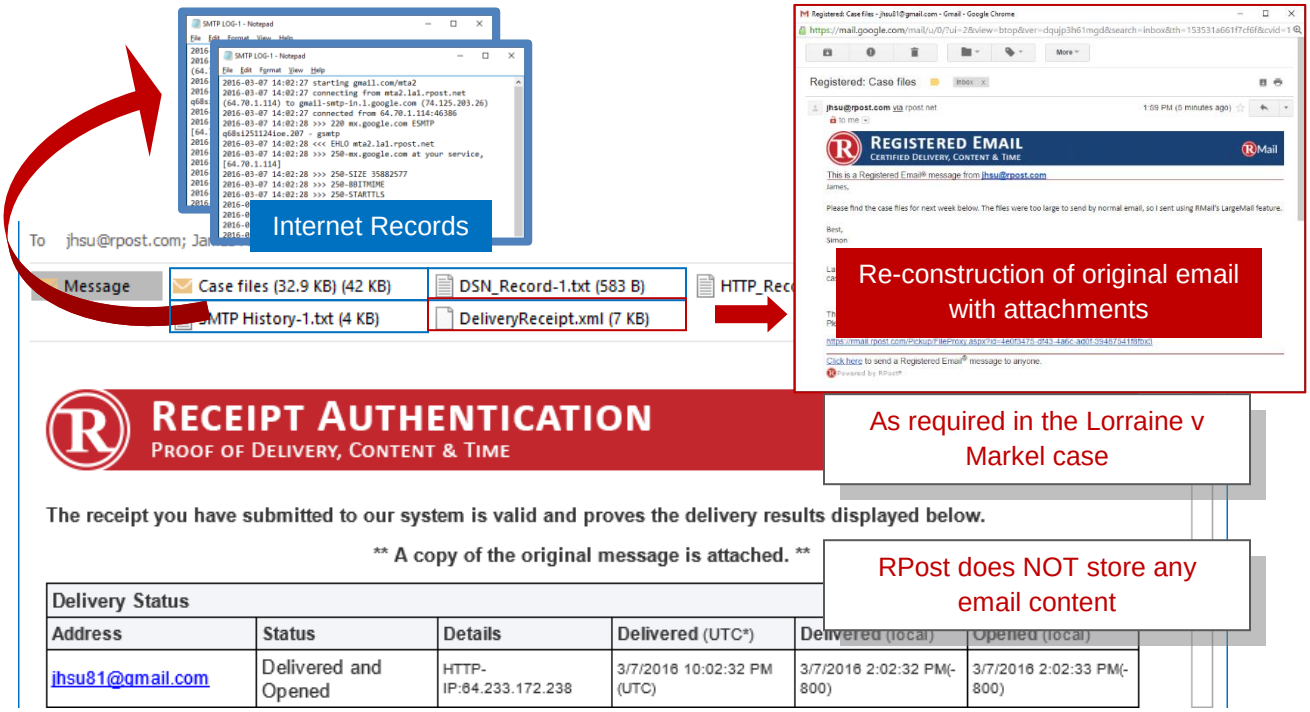
The Registered Receipt record is a standalone record. All transaction metadata – the data about the data transmission needed to reconstruct and authenticate the original message content, attachments, uniform government times of processing, sending, and receiving, internet forensics with cryptographic codes to ensure authenticity of all of this data -- are embedded encrypted (note C above) within the receipt itself. The RMail service does not store any of this information and cannot by itself (without the Registered Receipt being returned to the RPost system) reconstruct the transmission. The RPost system provides a

mechanism to authenticate the receipt and reconstruct the authenticated electronic original.

Verification of a Registered Receipt Record

The Receipt cryptographically associates the content with the delivery analysis, as well as uniform time stamps of sending and receiving, and then renders the entire 'Receipt' record resistant to tampering, verifiable, and able to re-construct an authenticated original email body text, attachments, internet forensics, official timestamps and delivery analysis.

The Registered Receipt record, when verified for authenticity, reconstructs from the transaction metadata the authenticated original content, attachments, timestamps, Internet forensics, and delivery analysis. This information is presented to the party inquiring about the message record authenticity, in the form noted below – as a Receipt Authentication email.



Real Estate Services Providers Council, Inc. (RESPRO®)
2101 L Street, NW, Suite 800 | Washington, DC 20037
p 202.862.2051 | f 202.262.2052 | info@respro.org