RMail™ By RPOST

Global Leader in Email Security

Seller Impersonation & Eavesdropping Detection

RMail.com

Explore Our Secure Email Services

- Email Privacy & Compliance
- Human Error Prevention & DLP
- Targeted Attack & Fraud Prevention
- Certified Proof of Content Delivered
- Outbound AI Security Stack

SHADDOCK NATIONAL HOLDINGS

Customer Stories

RPost was selected to replace one of the top leaders in the email encryption industry. With lightning speed, RPost developed and deployed a customized solution based on our wish list for detecting possible anomalous email activity. RPost exceeded our expectations and turned our wish list into a reality. With RPost's advanced eavesdropping detection technology, Shaddock National Holdings now has a crucial new tool to detect and thwart wire fraud attempts before they can cause any harm, a game-changing solution to protect our business and customers.

California R&D | **70+** Patents | **100%** AI-Infused | **190+** Countries

www.RPost.com

RMail By RPOST

Specialized Email Security Solutions Tailored to Combat Title Industry Threats

We're helping many of the largest title agencies in the U.S. detect and prevent key threats, including:

» Cybercriminal Eavesdroppers

In compromised real estate agent email accounts. RMail continuously monitors outbound email traffic for anomalies, providing early warning signs of compromised accounts. By catching cybercriminal activity in its early stages, title agents can drive proactive fraud management policies preempting fraud attempts and maintaining strong security hygiene within your agent ecosystem.

» Seller Impersonation Fraud

Speed is critical in identifying these threats. Our clients have reported catching impersonators within minutes of receiving new orders from agents. With real time monitoring in place, title agencies are finding it to be one of the few solutions capable of stopping these criminals before any funds are misdirected.

» Payoff Fraud, Construction Disbursement Fraud, and Lender Fraud

We recently partnered with ALTA to share insights on how our technology helped one of our customers detect a fraudulent lender, exposing a cybercriminal operating out of Moscow.

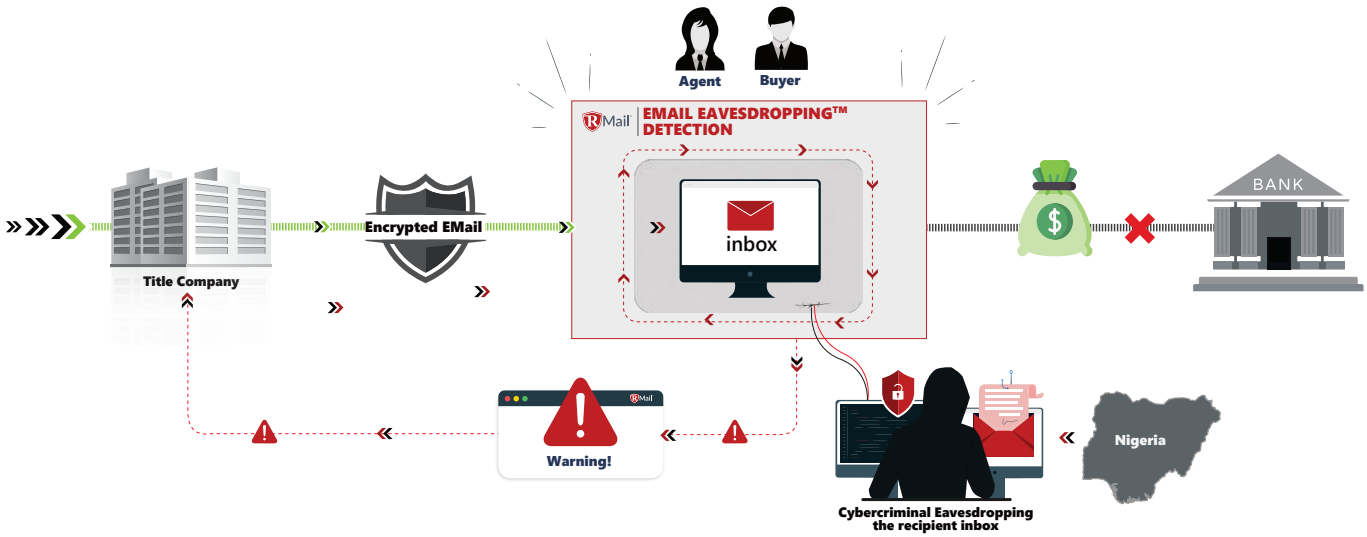
Seeing the emails were opened in Russia was an immediate red flag. I've been in the title industry for 30 years and haven't experienced this type of fraud.

Paul Hofmann,
Owner

AEGIS LAND TITLE GROUP

Cybercriminal Email Eavesdropping Detection

RMail's AI-infused email security technology is designed to detect anomalous activities in outbound emails for early detection of BEC and other sophisticated cybercrimes in progress. This provides the sending organization with real-time security intelligence, allowing them to implement proactive fraud prevention policies.



How the Anatomy of a Common Cybercrime Unfolds in the Real Estate Industry?

1. A cybercriminal gains access to a compromised email account, in many cases of a real-estate agent.
2. The cybercriminal monitors for important closing information.
3. The cybercriminal waits patiently for the perfect time to send a carefully constructed email to the buyer with fraudulent wire instructions.
4. The recipient sends payment to the cybercriminal account thinking it was the sender.
5. When the sender follows up with the recipient about the payment, they reply that they already sent it. And just like that, the funds are gone.

Email Eavesdropping™ Alerts for Advanced Fraud Detection

Email Activity Report

Email Eavesdropping™ Alert

Sender: Amy@TitleCompany.com

Original Recipient : James.Realtor@RealEstateBrokers.com

Security:	Red
Opens:	3
Locations:	2

Email Age: 15 days 1 hour 4 minutes

Pre-empt cybercrime.
After the hook is in, before the steal.

Risk Details: All Activities

Time (UTC)	Activity	Location	Country	Network Addr.	Network	Risk
09/15/2022 08:12:48	Open (VPN)	Ikeja, Lagos	Nigeria	41.67.191.255	Netcom Africa	Red
09/13/2022 17:06:22	Open	Boston, MA	USA	94.92.53.178	Verizon	Green
09/13/2022 12:54:18	Open	Boston, MA	USA	94.52.53.178	Verizon	Green

Original Message Details

Subject: WIRE INSTRUCTIONS FOR CLOSING
Original Send Time: 09/13/2022 03:20:00 UTC
Transaction ID: A4BD52B62EE9862A5FDDB8F336A99E2D69FEF54A

Metadata:

[IP Address: 41.67.191.255] [Time Opened: 09/15/2022 08:12:48 AM] [REMOTE_HOST: 192.168.10.153] [HTTP_HOST: open.r1.rpost.net] [SCRIPT_NAME: /open/images/LGy25hw0Z65CNLyOLYzCLCuMKdk95gm4vir26bBCMDIx.gif] HTTP_ACCEPT:*/* HTTP_ACCEPT_ENCODING:gzip, deflate HTTP_HOST:open.r1.rpost.net HTTP_USER_AGENT:Mozilla/4.0 (compatible; ms-office; MSOffice 16) HTTP_X_FORWARDED_FOR:183.82.2.55 HTTP_X_FORWARDED_PROTO:https HTTP_X_FORWARDED_PORT:443 HTTP_X_AMZN_TRACE_ID:Root=1-632d2601-68f7d3e527e10ac35f151b35 HTTP_UA_CPU:AMD64 Accept: */* Accept-Encoding: gzip, deflate Host: open.r1.rpost.net User-Agent: Mozilla/4.0 (compatible; ms-office; MSOffice 16) X-Forwarded-For: 183.82.2.55

RPost patented (rpost.com/patents) including US patent applications 17663425, 63/201,857, 63/366,685, 63/366,661 and other applications.

(M) = activity determined to be on a mobile device.
(N) = content delivery network delivered email data to viewer via webmail client.
(V) = activity was detected at an anonymizing VPN endpoint location.
(S) = activity determined to be caused by a server.
(E) = activity determined to be an expert user.
(R) = activity determined to be related to a Russian-centric device.
(K) = activity determined to be related to nefarious behavior of masking data.
(B) = activity determined to be related to automation scripts or bots.
Location = registered location of the detected network.
Network = registered network associated with the internet protocol.
IP Addresses: The "." are replaced with "-", to convert them to a valid IP, change these symbols back.

If the RMail **active threat hunting** technology identifies unusual activity patterns, RMail generates an Email Eavesdropping™ instant alert, and notifies in real-time IT admins (and optionally senders) with forensic details.

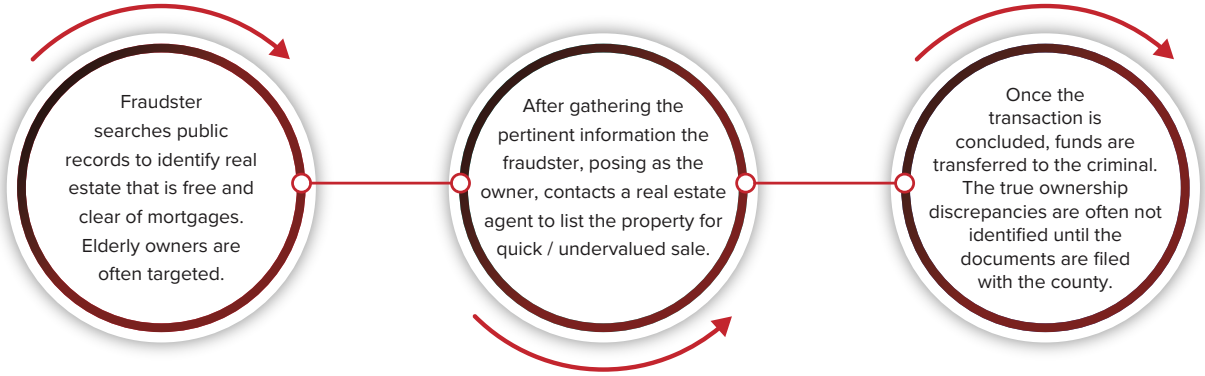
BEC lures start with cybercriminals targeting their victims by eavesdropping on email from sender to recipient, to siphon off email, analyze it, copy it with slight modifications (e.g., payment instructions), and then pivot replies so they route in a loop back to the cybercriminal.

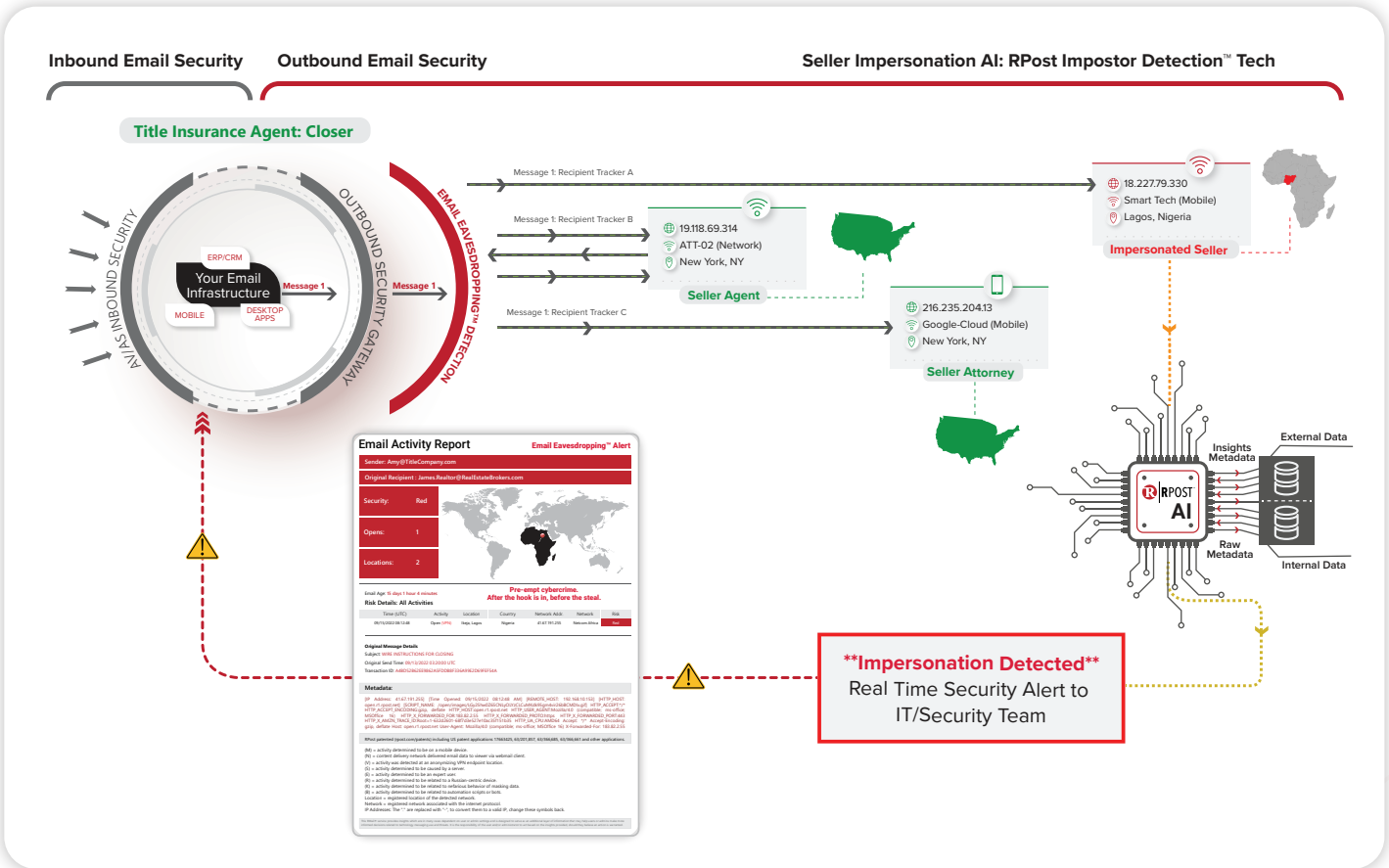
With Email Eavesdropping™ alerts, every email sent out of the organization has every activity associated with it analyzed forensically, for a period of time. These alerts include all the email forensics so that IT security specialists can validate and take immediate action, **before the cybercriminal lures users into mis-wiring money to the criminal's bank.**

RMail By RPOST

Seller Impersonation AI: RPost Impostor Detection™ Tech

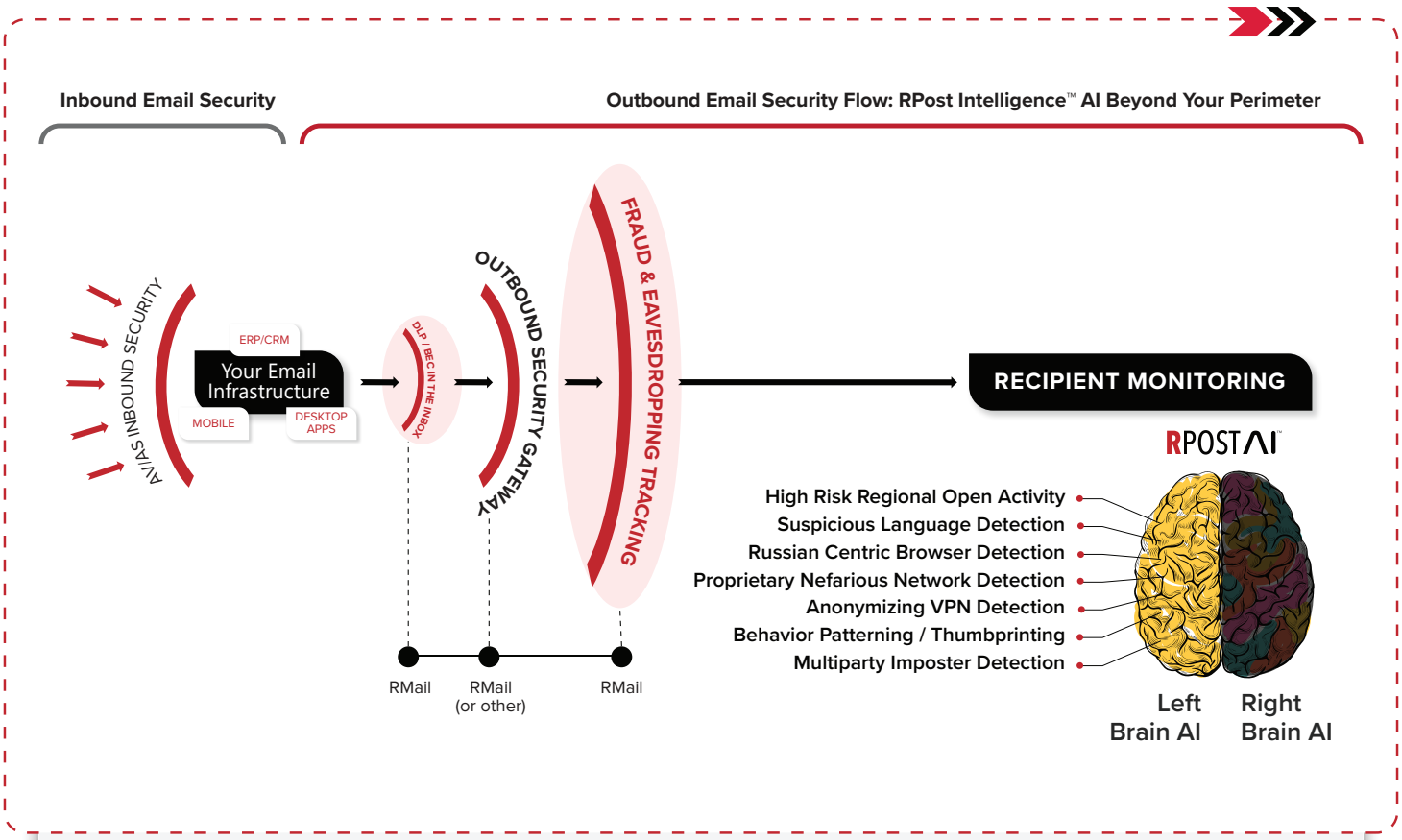
Traditional inbound email security solutions are typically ill-equipped to detect vacant lot fraud. This type of fraud doesn't trigger the usual red flags such as email spoofing or thread hijacking. To bridge this gap, RMail technology is designed specifically to identify the unique patterns and behaviors characteristic of this type of fraud, empowering organizations with robust forensic insights that allow them to take preemptive measures to protect their customers.





Seamless Integration I AI-Powered Intelligence

RMail Outbound Cloud Security Platform most often acts as an extension of one's existing inbound email security filters and outbound DLP services, with specialized Email Eavesdropping™ protection, elegantly easy and automated email encryption, and more.



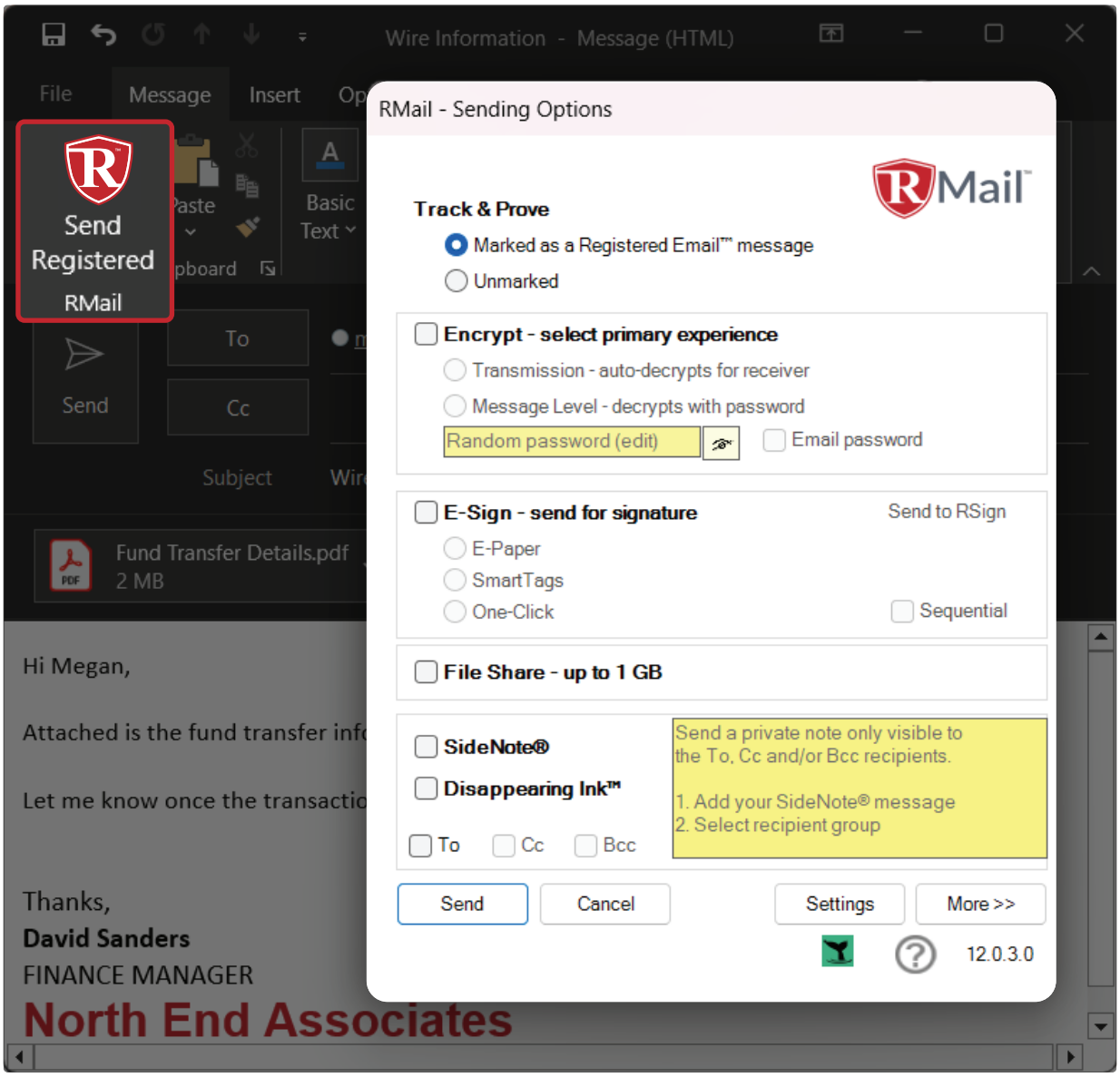
RMail services detect when a message should be sent encrypted and automatically transform it into a secure message that recipients can view with ease.

With Email Eavesdropping™ threat hunting, senders have peace-of-mind that they will be alerted in real time if a cybercriminal has compromised their recipient's email inbox, which is often the main step in lures leading to mis-wires.

RMail then sends aggregate Email Eavesdropping™ red-alerts to administrators and, if desired, to their managed security service provider as well.

RMail By RPOST

Optional Outlook Plugin with Advanced Features



RMail installs seamlessly into Microsoft Outlook, Gmail, Salesforce and more to empower users with its full set of email security, DLP, privacy compliance and productivity tools at the click of a button.

RMail By RPOST

Email Privacy & Compliance

SMARTR Email Encryption

Dynamically adapting encrypted email ensures elegantly easy; simple for recipient means happy sender. Far beyond opportunistic TLS, RMail encrypted email service smartly adapts to provide peace-of-mind with end-to-end encryption, secure file sharing, auditable proof of fact of GDPR and HIPAA privacy compliance, email thread security monitoring, and more.

Human Error Prevention & DLP

Mutating the DNA of Data Leaks

Automatically sensitize users of their need to treat certain messages differently, seamlessly and in the flow of email and work, with in-the-moment-of-sending, bite sized insights and alerts. Empower your people and prevent data loss with AI-Infused and automated rules-based email compliance and security recommendations.

Targeted Attack Pre-emption

Intercepting the Human Instinct to Please

Nip cybercriminal-induced mis-wires (a/k/a wire fraud) with real-time alerts that expose whose email account is being eavesdropped on, which email addresses have tricky lookalike domains, and when a reply is about to be hijacked--must-have additional layers for your Business Email Compromise defense. Outbound Pre-Crime™ email security at its finest!

Certified Proof of Content Delivered

Proof of Who Said What When, by Email

Gain insights of the overall journey of your email, how popular who read what when, and receive forensic certified proof.

Outbound AI Security Stack

Perfect Harmony, Enhance the Outbound

Keep your existing inbound email security – and even your outbound DLP if you so choose. Add RMail outbound security gateway, in-the-inbox integrated cloud email security, and in-the-ether eSecurity content controls: all, some or one. RMail harmoniously extends your existing email security systems, adding elegantly-easy encryption user experiences, unique BEC targeted attack detection, and more, with AI DLP automation.

Why We Are Unique

Our features provide the best user experience. Our prices make us the most affordable. And our services connect elegantly inside your existing email programs and business systems.

Breadth of Services

RMail empowers you; all of the functionality you need, all in one installation onto the platforms you're already using -- email encryption, certifi ed proof, AI-infused human e-security error prevention, in-the moment personalized eSecurity training,and much more.

Simplicity

We understand that the power of eSecurity technology resides in user adoption. That is why RMail is built with AI that automatically sensitizes users to today's eSecurity and e-compliance needs, subtly nudging them to make the right email-related eSecurity decisions. Securing your business has never been easier.

Legal Proof®

Each message comes with a Registered Receipt™ email record; the global standard for court-accepted, timestamped proof of secure delivery of emails — and its attachments. This record is durable (it may be forwarded, retaining its self-authenticating integrity), and is self-contained (it does not require any other record to be stored anywhere).

Friendlier Service

Excellent technology is key, outstanding service is gold. Getting both in a single package is pure bliss. Our teams are more knowledgeableand friendlier to work with. That is why our customers rate us with 99% satisfaction scoresand 5-star accolades.

Thank you, to the more than **25 million people** the world over, who have put their trust in our team and technology, **since 2000.**

USDA Allianz BT Claro GT GreenbergTraurig THE DOCTORS COMPANY Coca-Cola AMERICAN EXPRESS UNITED NATIONS

RMail™ By RPOST

Our Clients

Allianz Direct

How Allianz Direct enhances data security, meets legal compliances, and protects from non-receipt claims cases with RMail® via the Registered Receipt™ that offers email delivery tracking and proof of record for each policyholder reminder and expiry notification sent.

London Mutual
Credit Union

How London Mutual Credit Union integrates RSign® into their business operations to reduce friction in managing the loan process, speed and optimize documentation and agreements, and close loans and other applications faster.

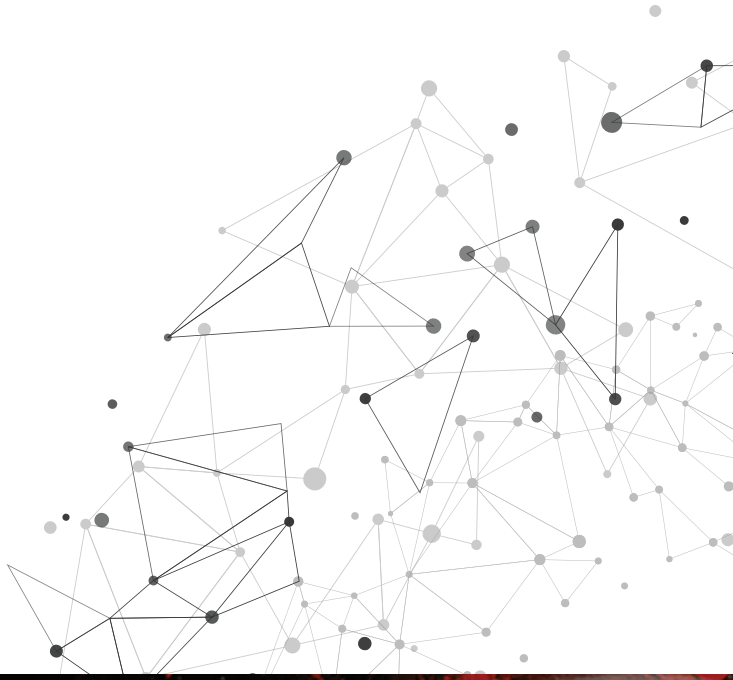
Shell Global

How Shell optimizes its trading and shipping operations by moving the critical, OTC petroleum product and derivative trade settlement notifications from e-fax to RMail's® Registered Email™ service to get the highest electronic evidentiary record of trade settlement delivery, content, and timestamp.

THE Coca-Cola COMPANY

How Coca Cola uses RSign® electronic signatures to lock in complex pricing for distribution contracts, resulting in speedy business and improved accuracy of price confirmations.

10,000 Customers strong & growing	**190+** Countries served daily	**Top 10's** Customers in many sectors	**90%** Recurring contracts	**70+** Patents



RPOST™

Contact us.

Mike Rooney
VP of Enterprise Sales
Cybersecurity & Digital Transaction Management
Mobile: (617) 777 3859

MRooney@RPost.com I www.RPost.com