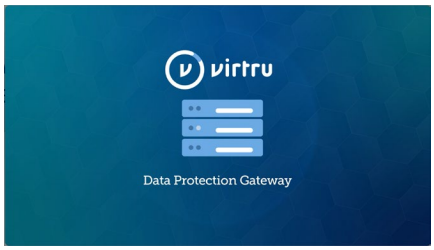
Total Rewards Statements Secure-Email Distribution FAQs

Here are the answers to some frequently asked questions about our secure email-distribution process.

How does Flimp securely distribute total rewards statements to employees?

Flimp partners with Virtru, a leading data-protection provider, to securely distribute statements to employees via encrypted email. Using Virtru's Data Protection Gateway, each email is automatically secured with advanced encryption and Data Loss Prevention (DLP) protocols to ensure the confidentiality of sensitive employee information.



This video explains more.

What is Virtru?

Virtru is a secure-email and file-sharing platform trusted by more than 7,000 organizations globally. It provides a secure wrapper around sensitive data—emails, attachments, and files—ensuring only intended recipients can access them. You don't need a Virtru account to open or reply to a secure message. Identity verification is quick and easy using existing credentials (Google or Microsoft) or by verifying through a secure link. Learn more at virtru.com.

Does the email come from Virtru?

No, the message will come from trs-distribution@flimp.net on behalf of the employer using Virtru's encryption platform. Virtru is the security layer, not the sender.

Do employees need to install any software to view their message?

Google Microsoft

No installation is required. To view a secure message, employees simply:

- Use their existing Google or Microsoft credentials or
- Choose to receive a one-time verification email and click the link.

Can an employee open their message if it was sent to a different email address?

Virtru uses email-based identity verification. The email can only be opened from the email address provided by the client.

Can employees reply to the secure message?

Employees can attempt to reply, however:

- They'll receive a bounce-back message from Virtru indicating the email could not be delivered.
- They'll also receive an automated response from trs-distribution@flimp.net informing them that replies are not monitored.

This safeguard is in place to protect employee privacy and ensure inquiries are routed to the appropriate internal team.

What happens if someone receives the wrong file?

All total rewards statements are protected with Virtru's Trusted Data Format (TDF) encryption. This technology enables Flimp to revoke access to any document at any time, regardless of whether it's been downloaded or shared. This ensures full lifecycle control over distributed data.

Is Flimp's secure-email distribution compliant with privacy regulations?

Yes, all communications are encrypted and sent through Virtru's Data Protection Gateway using military-grade encryption. This method is fully compliant with:

- HIPAA
- GDPR
- PCI-DSS
- CCPA
- FTC Safeguards Rule
- And other major data-protection standards

What certifications does Virtru hold?

Virtru meets rigorous global security standards and holds the following certifications:

- SOC 2 Type II
- FIPS 140-2 Validated
- FedRAMP Authorized
- ANSSI Certified
- G-Cloud 13 Framework Approved
- Cloud Security Alliance Member

Learn more in the Virtru Compliance Overview.