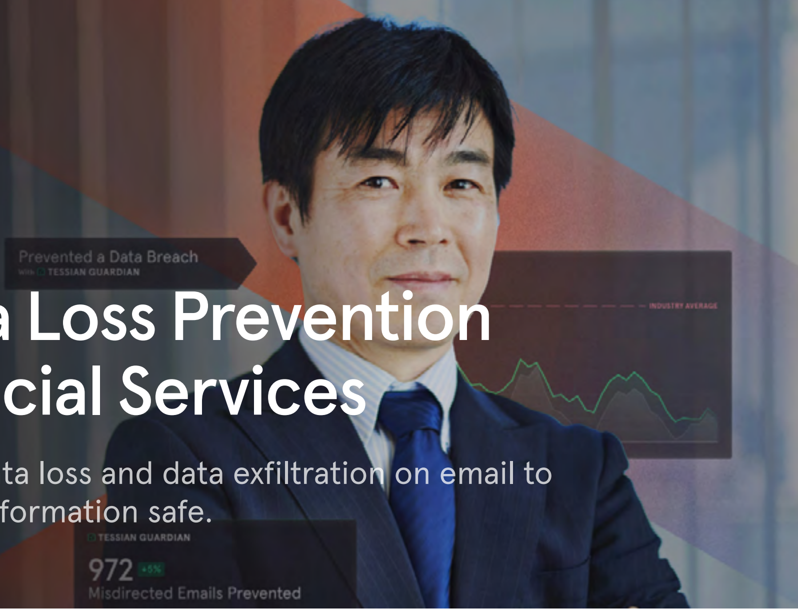
TESSIAN

OUTBOUND EMAIL SECURITY

An Essential Part of Data Loss Prevention (DLP) Strategies In Financial Services

Tessian automatically prevents both accidental data loss and data exfiltration on email to help ensure financial institutions keep sensitive information safe.



TRUSTED BY GLOBAL-LEADING FINANCIAL INSTITUTIONS

EVERCORE BDO PRUDENTIAL affirm Schroders

GOCARDLESS JTC

PREVENTING DATA LOSS IS TOP OF MIND FOR SECURITY LEADERS IN FINANCIAL SERVICES

800
misdirected emails are sent every year in organizations with 1,000+ employees

34%
of employees working in the legal sector admit to exfiltrating data before leaving a job

27,500
unauthorized emails are sent in organizations with 1,000 employees per year

85%
of security leaders say rule-based DLP is admin-intensive

Download The State of Data Loss Prevention in Financial Services →

WHY FINANCIAL INSTITUTIONS CHOOSE TESSIAN OVER OTHER SOLUTIONS

No Rules Required

Unlike other DLP solutions, Tessian doesn't rely on manual data classification, pre-defined rules, or blacklists. **You can't define and predict human behavior with rules.** Instead, powered by machine learning, Tessian maps employee relationships to automatically determine whether an email is suspicious or unusual.

This means effective, continuous, *adaptive* email security that's hands-off for security teams.

Unique Risk Insights

Security teams can easily view trends over time to identify their most risky users **without** looking through spreadsheets containing thousands of events. With these insights, customers can identify potential insider threats or negligent employees and take targeted action directly in the portal and outside of the portal before it's too late.

Learn more about Tessian Human Layer Risk →

Education and Awareness

When Tessian detects misdirected emails, misattachments, or data exfiltration attempts, a warning message is triggered, explaining exactly why the email was flagged in plain English. This helps reinforce existing policies around data handling, bolsters security awareness training, and drives employees towards safer behavior on email long-term.
Low rates of false positives mean warnings are helpful, not annoying like standard pop-ups.

DEPLOYS WITHIN MINUTES → LEARNS WITHIN HOURS → STARTS PROTECTING IN A DAY

WHAT OUR CUSTOMERS ARE SAYING:

Schroders

5500 EMPLOYEES

"We trust Tessian's technology to flag when an email is malicious or anomalous, and we trust our employees to interact with the warnings and do the right thing. And, we can actually see that threats are being prevented. We can see it works. But, without any investigation and no noise."

Rob Hyde
CISO
SCHRODERS

"You can't have one rule for all use cases or just block by default. Tessian allows us to take a more nuanced approach and leverage different controls for different departments. By addressing specific risks, for specific teams, we can manage risk better."

Elsa Ferreira
CISO
EVERCORE

EVERCORE

2000 EMPLOYEES

intertrust
GROUP

4500 EMPLOYEES

"Week to week we can see who's triggering the most warnings related to misdirected emails or unauthorized emails. This gives us a chance to re-educate them. The good news is, we never see the same name two weeks in a row. That shows us that the platform is working. It's resonating, it's changing behavior, and decreasing our level of risk."

Katerina Sibinovska
CISO
INTERTRUST

"We love Tessian because it's very low-impact and doesn't obstruct employees' work and It delivers with accuracy. Our IT team likes the noise-to-value ratio."

Ray Chery
SVP AND CO-HEAD OF SECURITY SOFTWARE
JEFFERIES

Jefferies

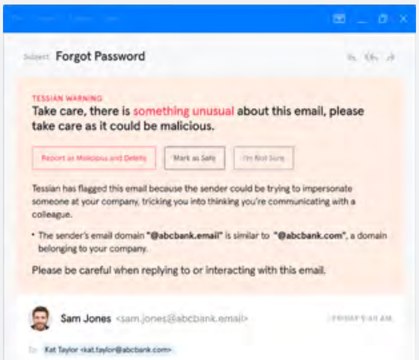
5000 EMPLOYEES

Man Group plc

1700 EMPLOYEES

"Tessian proved its value after a few weeks of being deployed firm-wide. For the first time ever, we now have visibility and control overinadvertent data loss through misaddressed emails and information being sent to unauthorized email accounts, both of which are key information security risks for our business."

Neil Wellard
HEAD OF IT
MAN GROUP



Subject Forgot Password

TESSIAN WARNING

Take care, there is something unusual about this email, please take care as it could be malicious.

Tessian has flagged this email because the sender could be trying to impersonate someone at your company, tricking you into thinking you're communicating with a colleague.

- The sender's email domain **"@abcbank.email"** is similar to **"@abcbank.com"**, a domain belonging to your company.

Please be careful when replying to or interacting with this email.

Sam Jones <sam.jones@abcbank.email> FRIDAY 9:41 AM

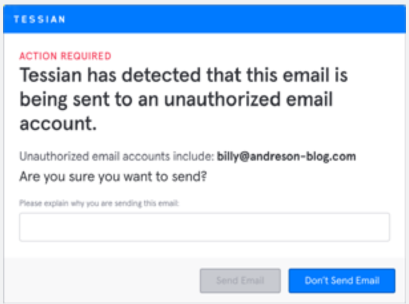
To: Kat Taylor <kat.taylor@abcbank.com>

PREVENT ACCIDENTAL DATA LOSS

Tessian Guardian

As misdirected emails and incorrect attachments are detected, employees are alerted in real-time with clear, simple explanations and precise reasons for anomalies and correct recipients are suggested. This way, they can correct the recipient(s) and review attachments before the email is sent.

LEARN MORE →



TESSIAN

ACTION REQUIRED

Tessian has detected that this email is being sent to an unauthorized email account.

Unauthorized email accounts include: **billy@andreson-blog.com**

Are you sure you want to send?

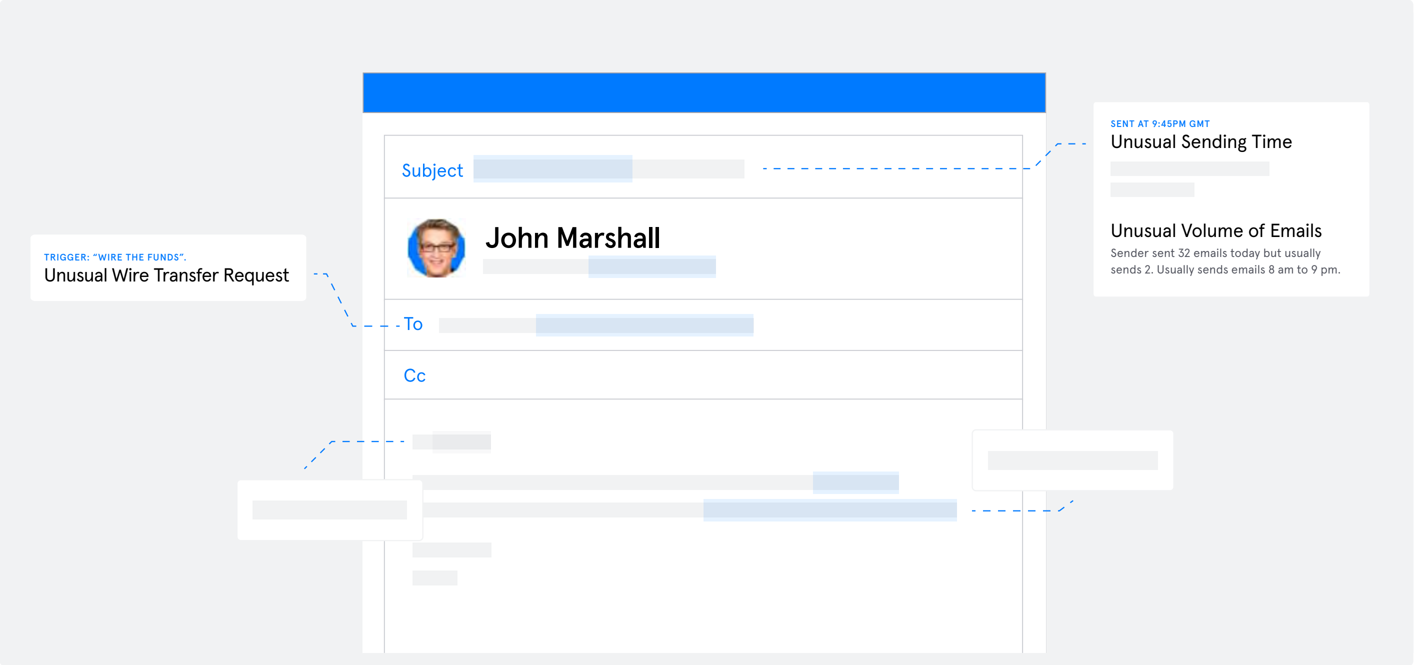
Please explain why you are sending this email:

PREVENT DATA EXFILTATION

Tessian Enforcer

Real-time warnings are shown to employees when data exfiltration threats are detected. Warning triggers can be tailored to suit your company's security policies and workflow requirements; employees can be warned, emails can be blocked, or activity can be silently tracked.

LEARN MORE →



TRIGGER: "WIRE THE FUNDS".
Unusual Wire Transfer Request

SENT AT 9:45PM GMT
Unusual Sending Time

Unusual Volume of Emails
Sender sent 32 emails today but usually sends 2. Usually sends emails 8 am to 9 pm.

See how you can turn your email data into your biggest defense against outbound data loss.

REQUEST A DEMO →

TESSIAN

Human Layer Security

TESSIAN.COM

Tessian's mission is to secure the human layer. Using machine learning technology, Tessian automatically stops data breaches and security threats caused by human error – like data exfiltration, accidental data loss, business email compromise and phishing attacks – with minimal disruption to employees' workflow. As a result, employees are empowered to do their best work, without security getting in their way. Founded in 2013, Tessian is backed by renowned investors like Sequoia, Accel, March Capital, and Balderton and has offices in San Francisco and London.