



Trustifi

Trustifi Case Study

Email Security Solution

Independent Financial Group Inc.



Independent
Financial Group, LLC

Independent Financial Group, LLC (IFG) adopts Trustifi's secure email solution, because Trustifi provides the security that its IT/security administrators sought, along with the simplicity that encourages user adoption.

Independent Financial Group, LLC (IFG) is an award-winning independent financial broker-dealer that operates in the brokerage and advisor space. Its team of 620+ independent financial professionals offers personalized services to individuals and institutional investors. Having integrated Trustifi into its existing email platforms in order to secure against email threat vectors, IFG can easily conduct secure email communications (both internally and externally) with its independent financial advisors and customers throughout the U.S.



***“With Trustifi,
you don’t have
to choose
between
security and
usability.”***

Mason Moore

IT Manager at Independent
Financial Group, LLC based in
Del Mar, San Diego, California

Email Threat Vectors Attack Your Weakest Link

Businesses are constantly being bombarded by malicious attack threat vectors that operate through email inboxes/outboxes.

Phishing, email fraud, malicious attachments, malware and ransomware operate via email with the objective of stealing money, data and damaging your reputation and brand.

Email attackers are very skilled at taking advantage of the weakest link in your organization – the humans and their emails.

Malevolent entities use a wide variety of ever increasingly sophisticated techniques to lure your employees and customers in order to attack your organization through email, while evading detection forever or at least until it is too late.


Mason Moore said, “As an IT manager with an extensive security service background, my department and I are responsible for the organization’s information security and availability. We take every possible measure to protect our own data and our customers’ data, including advisory data, financial data, account numbers, personally identifiable information (PII) and more.

Regarding email, we were particularly aware of malicious actors making data exfiltration attempts and attempting to send malicious payloads to our users and clients.

Another major concern are the spoofing attempts that we experience by malicious entities who send unauthorized emails (internal and external), while masquerading as a different person and/or organization in order to get one of our users to act on them.

Previously, we were using a very well known email security platform and a lot of this stuff got through. This meant that we had to invest intensively in whitelisting and blacklisting, in order to subvert some of the machine learning of that platform. This was not ideal for us.

Therefore, we were looking for another provider for our email security filtering.”



As an IT manager with an extensive security service background, my department and I are responsible for the organization’s information security and availability.

Multi-step Procedures Deter Adoption

"We were having trouble with human compliance, especially in regard to external mails coming into the organization," says Mason Moore, IT Manager at Independent Financial Group, LLC.

"We found that Trustifi security has been above and beyond what we expected."

"We initially started using Trustifi just for its email encryption features, because our previous solution's email encryption feature was a pain, making it difficult for our advisors to communicate with us and for them to communicate with their clients.

We have regulatory bodies that we must answer to. Our advisors not only have to answer to them, but also have to follow our protocols and guidelines intended to keep them safe. We found that our IT/security team had to invest significant efforts to instruct our advisors about the procedures, protocols and guidelines for using these encryption features in order to send PII.

Still, we found that many of them were silently abandoning these security procedures, so that we repeatedly had to reiterate the procedures and try to convince them to continue using it.

Despite these efforts, there was no other way to ensure the protection of our sensitive client data than to conduct continuous surveillance of the messages coming in and out of our organization."

We found that people sending encrypted emails using other email security solutions were confused and tended to abandon it quite quickly.

Trustifi Provided the Security and Deployment Simplicity We Were Seeking

Trustifi's email security services feature a comprehensive suite of email tools for advanced threat protection, data loss prevention and enterprise email encryption.

- Trustifi –
- **Provides visibility into all email-based attacks.**
 - **Enables email authentication for both inbound and outbound email.**
 - **Protects against data loss.**
 - **Enables rapid response to threats and attacks.**

Advanced Threat Protection

- Malware and ransomware virus detection, prevention, protection and alerts
- Spoofing, phishing and fraud detection
- Whitelisting and blacklisting options

Data Loss Prevention

- 100% compliant with HIPAA/HITECH, PII, GDPR, FSA, FINRA, LGPD, CCPA and more
- Realtime knowledge about when emails have been received, opened and read with certified delivery and tracking
- Two-factor authentication on the recipient (even without registering)

Encryption

- NSA-grade end-to-end email encryption, with full inbound and outbound protection
- Secure mobile relay for full protection on any device
- Recall, block, modify and set expirations for already sent and delivered emails

Trustifi makes it easy for your IT security staff to get the security they need, including alerts, traceability, monitoring and awareness, while being straightforward, transparent and simple enough for end users to apply all this security at the click of a button.

Regarding setup and configuration, Mason Moore said, "We found that once Microsoft 365 Data Loss Prevention (DLP) was set up, it was not bad. However, we found its implementation (meaning installation and configuration) to be clunky and vague, making it difficult to properly configure rules, conditions and alerts.

One example is when we set up alerts to notify us that a user's internal email box was forwarding to an external recipient. This was easy enough. But when a rule was triggered, it required us to go through multiple steps and screens in order to investigate the incident.

Even though we initially engaged Trustifi because of its outbound features, encryption and DLP, one of the nicest features of the Trustifi platform is its immediate visibility into a message's authenticity fails and successes. From a single initial view, we are able to investigate and troubleshoot security incidents.

As mentioned, the initial setup of Microsoft 365 DLP is simple. However, configuring its conditions to meet our exact environment was quite tricky, especially trying to prevent it from falsely flagging email content as PII. It regularly mistakenly encrypted content and sent it to recipient organizations, who would then complain about receiving unexpected encrypted files."

***"With Trustifi,
we saw a huge
decrease in false
positives."***

Other customers of ours have said, "Unlike its competitors, Trustifi's solution was the ideal balance of user-friendly and advanced security technology. Trustifi excels in these situations. Its deployment is simple and only takes less than fifteen minutes. In the rare occasion that the infrastructure was more complex, Trustifi took immediate action to remotely rectify any roadblocks."

Trustifi is Easily Deployed with –



Gmail/G Suite
Add-in or Relay



Outlook/O365
Add-in or Relay



Any Email Server
Relay

***Other customers of ours
have said, "Unlike its
competitors, Trustifi's
solution was the ideal
balance of user-friendly
and advanced security
technology."***

Trustifi's Simple User Interface Encourages Users to Adopt Willingly

"We were searching for a service that would make it easier for recipients to access secure messages and easier for the sender to securely package them," said Mason Moore.

Mason Moore described how they operate and the previous email security solutions they were seeking to replace.

"Our business typically requires that everyone conduct most of their work in another system that does ticketing, routing, documents, commission, tracking and so on. Various circumstances arise where our users simply want to send a document by email that must be encrypted, such as audit info that contains PII to a third-party agency. Another example is when some of our onboardings consist of a few thousand accounts at a time. Previously, we used to transition that paperwork over encrypted faxes over Internet."

"Now, because of Trustifi, it is so nice and easily accessible to use encrypted email as a side channel for sending this information. Just open Outlook (for example) and do it."

In 2017, I realized that the platform was ideal for another email security situation. Back then, we were routing all our client messages through a **different email security** server that we hosted on-premises. We were having connectivity issues at that location, as well as issues accessing the email because of account issues. We started searching for another security solution because of so much **pushback from the email users.**

When we initially engaged Trustifi for outbound emails, we didn't even know that Trustifi had an inbound component. We also didn't realize that Trustifi was able to accommodate us without any adjustment to the contract. We later were able to easily get it up and running in order to replace our existing email security services.

We no longer had to spend lots of time explaining the security procedures, convincing users to adopt them, monitoring alerts when users aren't applying security measures and then investigating the security issues that would arise because they didn't use them."

Mason Moore said, ***"After we started using Trustifi we have seen an increase in the adoption and utilization of email encryption from the home office."***

Trustifi is Click-of-a-Button Easy

End-to-end secure emails are sent and tracked with the click of a button, and easily opened, read and returned.



Email Encryption Made Easy

Using Trustifi's email solution, administrators can create rules that automatically detect and encrypt messages that contain sensitive information. For the financial industry, these rules can detect PCI data or certain keywords, such as revenue or credit card information. When the system scans an outgoing email and finds a keyword or rule, the system subsequently encrypts and locks the email without any input from the user.

This ensures that sensitive data and attachments are not at risk before they reach their intended target. Our optical character recognition (OCR) technology can recognize checks, credit cards, bank statements and more. Your PCI data and reputation are not at risk and your organization can avoid hefty fines from government bodies.

Administrators can receive notifications when the system follows the rules in place and successfully encrypts an email with PCI data. Artificial intelligence has changed the game for email cybersecurity. Trustifi also has a multi-factor authentication system to identify the receiver of the email. These extra protections help to ensure that your employees keep confidential and sensitive information safe from hackers.

Other Great Features That Users Like

When you choose Trustifi, you are getting a holistic email security solution – not just email encryption.



No Special Passwords

“One of the main features that our email users liked is not having to deal with a separate login. Our previous email encryption service required them to enter a complex password every time they wanted to send an encrypted message.

With Trustifi you simply open your email application and press a button to encrypt/decrypt email sending/receiving.

No forced registration for recipients”



Adding Other Recipients to an Encrypted Email Thread

“Let’s say you’re corresponding with multiple people using encrypted emails. Other email platforms do not allow you to add another recipient to the email trail. This means that corresponders had to start a new email thread in order to add another recipient to the encrypted email thread.

Trustifi automatically handles all this for you, so that you can simply add another recipient who becomes part of the secure correspondence.”



Recalling/Changing Emails

When you want to recall an email, the traditional method is that you send another email saying “please don’t read this email”. With Trustifi, you can actually replace the email and/or its attachment, track it and do all this without involving the recipient.



256-Bit AES Encryption

NSA grade protection over your data and files

Extra Security Features

- One time access to files/emails
- Block access to print files
- Delete or edit messages after they have been sent

Inbound Protection

Stay protected from malicious links and files, viruses, phishing and spoofing attacks, ransomware attacks and even Spam.

Multi layered 360° Protection

Multi-Factor Authentication

on the recipient- You can choose to lock an email by adding a pin or a question that can only be unlocked by the intended recipient for an extra layer of protection

No Log-in Portal or Account Necessary

one click authenticate and decrypt allows your recipients to open your emails and also reply encrypted without ever having to sign up or login to anything



Contact Trustifi today to discuss how to secure your organization's sensitive data with an easy to use email security platform that promotes productivity

www.trustifi.com

1-844-235-0084