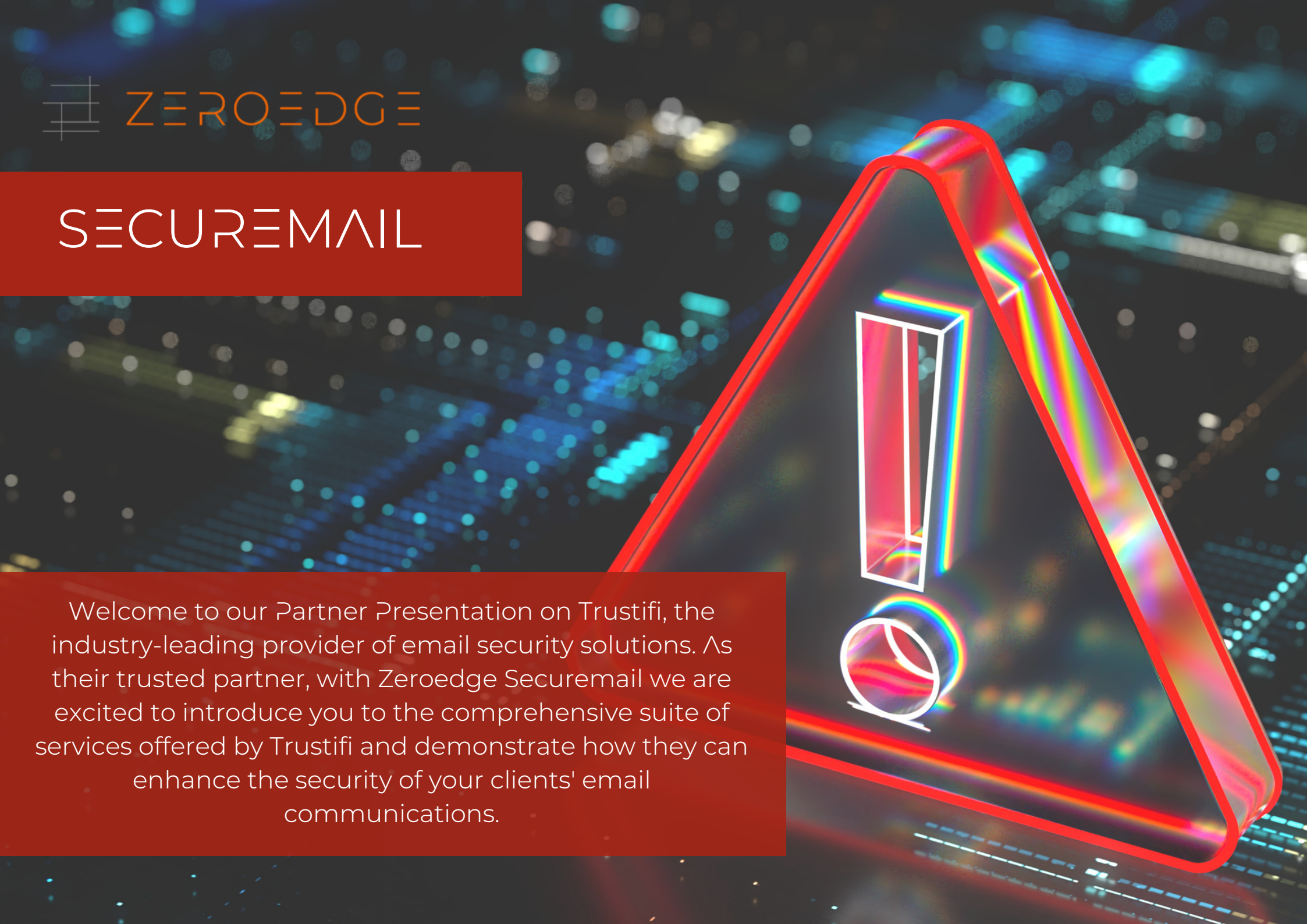
ZEROEDGE

SECUREMAIL



Welcome to our Partner Presentation on Trustifi, the industry-leading provider of email security solutions. As their trusted partner, with Zeroedge Securemail we are excited to introduce you to the comprehensive suite of services offered by Trustifi and demonstrate how they can enhance the security of your clients' email communications.

ENCRYPTION

AES 256-bit encryption secures your PHI data at rest, in storage, and in transit, rendering it unreadable to anyone but the sender and verified recipient. Secure mobile relay ensures protection on any device.

ADVANCED THREAT PROTECTION

Trustifi's AI engine scans all inbound emails in real time for targeted threats such as phishing and ransomware. Eliminate any malicious emails automatically before they reach your users' inbox.

REPORTING

Easily demonstrate compliance by generating reports of the use of encryption to secure data, including who sent and received encrypted emails, when, and from where.

DATA LOSS PREVENTION

1-Click Compliance™ employs a sophisticated rules engine to automatically encrypt sensitive email content, ensuring your data stays secure even if a user forgets to encrypt it.

MAIL DELIVERY TRACKING

From within your native email client, use the tracking features to confirm the delivery status of your emails, recall and edit messages even after sending, and set email expiry dates. Certify email delivery and tracking.

KEY FEATURES OF OUR LAW FIRMS SOLUTION

Trustifi provides a complete, all-in-one email security platform to protect law firms against advanced email threats. Trustifi blocks data loss, ensures compliance with data regulations, and protects against phishing attacks, ransomware, business email compromise, and more.

PROTECT YOUR CLIENTS AND ENSURE COMPLIANCE

Trustifi ensures that your client's personal data is fully protected, with granular data loss protection policies that ensure any personal, financial, or sensitive information included in or attached to an email is automatically encrypted. Administrators can set granular policies to govern encrypted data, with full control and visibility for end users over who can access encrypted email messages. Trustifi's 1-Click Compliance™ ensures full compliance with HIPAA/HITECH, PII, GDPR, FSA, FINRA, LGPD, CCPA, and more with just the click of a button.

ALL-IN-ONE EMAIL PROTECTION

Trustifi provides total protection for email. Inbound email is scanned for malicious content in real-time by powerful AI engines, protecting organizations from spam, malware, viruses, phishing, business email compromise, and ransomware. Protection extends to the email inbox, with real-time threat scanning of links and attachments even after email delivery. Outbound messages are protected with secure AES 256-bit NSA-grade encryption, ensuring sensitive data and attachments are always kept protected from malicious threat actors.

EASY-TO-USE ENCRYPTION AND END USER CONTROL

Trustifi's encryption process is totally seamless and incredibly easy to use. Users can send encrypted email with the click of a button, with full visibility over who has opened email messages, and extra controls, including the ability to unsend email and revoke access to malicious email messages. Unlike other encryption platforms, when you receive an encrypted email with Trustifi, you don't need to create a new account or log into a cumbersome secure web portal. You can see the message straight from your inbox with secure two-factor authentication.

Email Encryption and Data Security for Healthcare Organizations

In recent years, healthcare organizations have been put under pressure to ensure the security of their patients' protected health information, or PHI. This includes medical histories, test results, and mental health information, as well as demographic and insurance information.

Due to the personal nature of this data, it's crucial that it be kept confidential to protect the privacy of the patients. Because this data is so valuable, it's a prime target for cybercriminals, who can sell PHI on the dark web or attempt to jeopardize it as part of ransomware attacks. Not only can this compromise the financial security of affected patients, but it can also lead to delays in them receiving treatments due to a lack of medical records on file.

As attackers find increasingly sophisticated ways to steal confidential information, healthcare organizations must be vigilant in deploying the correct preventive security measures to protect that data. Encryption is one such measure. Encryption ensures that even if a cybercriminal manages to gain access to email records containing sensitive information, they won't be able to decipher the data within those records.

HOW TRUSTIFI PROTECTS HEALTHCARE IN THREE STEPS

Trustifi is a market-leading encryption provider that helps organizations to secure their email content via powerful AES 256-bit end-to-end encryption. Trustifi's solution is easy to deploy, easy to use for both senders and recipients, and—crucially—enables "one click" HIPAA compliance.

1

With just one click, send secure, HIPAA-compliant encrypted emails from within your regular email client to any recipient—even if they aren't using Trustifi. Leverage advanced features such as certifiable proof of delivery, message recall and modification, and message expiry dates, so that you know straight away when emails have been received, opened, and read. Leverage two-factor authentication for an added layer of security between a potential attacker and your data.

2

Use Trustifi's 1-Click Compliance™ feature to eliminate the complexities of maintaining and proving compliance with your regulatory bodies, while ensuring your data remains secure. Simply select with which standards and data loss prevention policies you need to comply, and Trustifi's AI engine will scan all outbound emails for sensitive content and encrypt them automatically. With the click of a button, make audits more efficient and mitigate human error. Compliance has never been easier.

3

Many encryption services fall flat by making it too complicated for end users to send and receive emails. But everyone has to use a solution properly for it to be effective. With Trustifi, users can send emails with the click of a button, and recipients can open them quickly without having to log into an external portal or create an account. Just enter your SMS authentication code, email PIN, or shared password, and you can read the message right there in your inbox.

EMAIL SECURITY FOR LAW FIRMS

Ensuring the protection of client data is one of the most important responsibilities of a law firm, or indeed any organization in the legal sector. It's vital, both legally and ethically, that when a client or customer entrusts you with their sensitive information, you keep it secure and protected.

But in the digital world, this is much easier said than done. Many of the digital technologies we rely on for instant communication and collaboration with colleagues and customers are inherently insecure, with a number of vulnerabilities that can be exploited by malicious actors looking to gain access to sensitive data. This is especially true when it comes to email.

With email encryption, you can set rules to guarantee that only your intended recipients can view email content and attachments and that email data cannot be accessed by third-parties while in transit. With Trustifi's sophisticated email encryption, you can set up automated data loss protection (DLP) policies that give end users the controls they need to protect client data and secure email access.

HOW CAN TRUSTIFI HELP SECURE LAW FIRMS?

Different methods of executing email encryption exist, but Trustifi's service provides secure, cloud-based end-to-end encryption for email.

With end-to-end email encryption, messages are secured at every stage of delivery and cannot be accessed by anyone other than the intended recipient. The crucial difference with end-to-end encryption is that the email remains encrypted even after it has been delivered. This means if the recipient is hacked or their mailbox is compromised, the email content is still safe and protected.

Ensure Legal Compliance

Email encryption is an important way to meet compliance regulations governing the usage and sending of private personal data. Trustifi's email encryption solution supports full compliance with legal regulations and helps you do the same.

It's one thing to be compliant, but equally important is proving you have acted in a compliant way.

1

Proof of encryption with time-stamped delivery

2

Reporting of when encrypted emails were sent and when they were opened

3

A way to preconfigure email settings so that sensitive data is automatically encrypted

ACCURACY AND DELIVERABILITY

In law firms, emails can often be extremely time sensitive, and delays between sending and receiving important information can have serious consequences. Because of this, it's crucial that encrypted emails are not only delivered to the correct recipient but delivered in a timely way.

It's important to send emails securely, but if the recipient never receives them or if they are blocked from being delivered, the service is ineffective. Trustifi's service ensures email deliverability and timeliness for both your users and your recipients.

EMAIL SECURITY, DATA PROTECTION, AND COMPLIANCE SOLUTIONS SPECIFICALLY DESIGNED FOR FINANCIAL SERVICES

Last year saw a dramatic increase in cyberattacks against the financial services sector, as cybercriminals capitalized on the volatility of the Coronavirus pandemic. In fact, according to recent research, 80% of financial institutions reported an increase in cyberattacks in 2020. These figures are expected to increase as we move towards post-pandemic life. Attackers will continue to employ new, sophisticated methods by which they can steal corporate data. This means that, whether you're a fund management service, an insurance company, a banking service, or a payment and settlement service, cybersecurity should be one of your chief concerns.

LTHE CRITICAL TAKEAWAYS FOR FINANCIAL SERVICES

In the financial services sector, email correspondence may contain sensitive personal or legal information, and it's often critical that this information be actioned within a strict deadline. For your brand to succeed, your clients must be able to trust you with the integrity of their confidential data this means that you must secure your emails.
The critical takeaways for financial services companies:

1. 86% of all breaches are financially motivated, and the financial industry is the second most common victim of security breaches
2. Implementing an encryption solution can help you meet many major data privacy standards, including PCI DSS (requirements 4.1 and 4.2) and GLBA, and prove your ability to keep customer data secure
3. A strong email encryption solution can secure sensitive data such as PII and NPI against unauthorized access via sophisticated email threats like social engineering, BEC, and ransomware, as well as island hopping attacks

KEY CHALLENGES FACING FINANCIAL SERVICES COMPANIES

1 DATA SECURITY

As a financial services organization, you're responsible for keeping your customers' confidential data secure at rest, in storage, and in transit. This means protecting it against potential cyberthreats. Money is the primary focus of the vast majority of system hacks, so it comes as little shock that the financial industry is the second most common victim of security breaches, closely following the healthcare industry. Personally identifiable information (PII), nonpublic personal information (NPI), and financial information (such as credit card numbers and account numbers) are lucrative targets for attackers, who either sell this data illegally on the dark web or hold it ransom until their victim pays a fee for its return.

Two of the most common attacks currently facing financial service organizations are spear phishing and ransomware. Spear phishing is a form of social engineering attack in which attackers disguise themselves as a trusted source, such as a colleague. The phishing emails attempt to trick their victims into handing over sensitive information, such as account credentials, or to click on a URL or attachment that will download malware onto the victim's device.

KEY CHALLENGES FACING FINANCIAL SERVICES COMPANIES

2 REPUTATION PROTECTION

Your customers trust you to keep their data safe. In fact, a recent survey found that 96% of American bank account holders describe security and fraud protection as being one of the most important features they look for in a bank.

Reputational damage is one of the key consequences of a data breach. If you fall victim to a cyberattack, you'll likely lose the trust of your customers. A strong encryption solution will help stop you from falling victim to an attack, thus preserving your reputation in the eyes of your customers.

Financial organizations often send emails containing PII, NPI, and other sensitive information such as account numbers, credit card information, insurance information, and credit scores. When sending these types of information, you need to be certain that the right person receives them. Multi-factor authentication (MFA) can be one weapon in your security arsenal. MFA requires recipients to verify their identity in two or more ways before they're granted access to the email's content.

KEY CHALLENGES FACING FINANCIAL SERVICES COMPANIES

3 COMPLIANCE

As a financial services organization, you're aware of regulatory standards with which you must comply in order to operate within the law. These regulations differ from country to country and from state to state, so it's important that you research which compliance standards are relevant to you. Data privacy standards typically affecting financial institutions include (but are not limited to) the following:

PCI DSS states that unencrypted credit card information should not be transmitted over open networks such as the internet and wireless networks (Requirement 4.1), and that organizations should never send unencrypted primary account numbers via end-user messaging technologies (Requirement 4.2). This means that your organization can send payment card information via email and still achieve compliance, as long as you encrypt that information.

The FFIEC provides guidance for organizations that want to be GLBA compliant. They state that "financial institutions should employ encryption to mitigate the risk of disclosure or alteration of sensitive information in storage and transit." This includes making sure your chosen encryption solution protects your data for as long as it needs protecting, i.e. that your subscription won't run out or expire. You must also manage your cryptographic keys properly. To ensure you're meeting these requirements, your chosen solution should be in line with the NIST and FIPS encryption standards.

HOW TRUSTIFI PROTECTS FINANCIAL SERVICES IN THREE STEPS

This feature enables organizations to become fully compliant with PII, HIPAA/HITECH, GDPR, FSA, FINRA, LGPD ,and CCPA standards. With a click of a button, Trustifi eliminates the complexity of compliance while ensuring that confidential data remains secure. Administrators can configure this policy from within the solution's management console.

Trustifi also provides advanced protection against inbound email threats, such as social engineering and ransomware attempts. It can filter out spam emails, which can clog up and slow down your users' mailboxes. Trustifi's AI Engine scans all inbound email communications in real time and rates each message according to its threat type and severity—these ratings range from "Authenticated" to such alerts as "Impersonation Attack" and "Spoofing Attack."

TO LEARN MORE

+41 91 695 09 80

SALES@ZEROEDGE.CH

ZEROEDGE.CH