SOLVING THE Encryption Conundrum in Financial Services
INTRODUCTION

Encryption has gone mainstream.

In March this year, WhatsApp announced that it would encrypt all users’ communications. Viber and Facebook soon followed suit. In one fell swoop, these three companies shifted the user base of strong encryption from what most believed to be whistleblowers and journalists to almost three billion people worldwide.

Meanwhile, government bodies are busy endeavouring to weaken strong encryption in the interest of national security as technology companies, opposed to such a precedent, are arguing that the privacy and the security of millions of innocent citizens would be at risk.

The encryption debate has captured the world’s attention. And coupled with the inevitability of another notable data breach, awareness of encryption as a tool to mitigate threat is at an all-time high.

What does this mean for FS?

Despite being one of the first industries to embrace a digital transformation agenda, the financial services sector continues to struggle in the race to deploy digital technologies in order to grab a bigger “piece of cake.” As competition from new, digital-first financial start-ups continue to grow; banking executives are focused on game changing digital solutions, such as encryption, to compete successfully. If you want to talk to your customers, the security has to be there. The better your security the closer you can be to your customers. In this whitepaper, we delve into the link between encryption investments to growth and customers.

Consider encryption a competitive differentiator.

Consumerisation of encryption is the driving force behind customer demand for secure digital communications, and as a result, increased expectations. The ease at which confidential information can be intercepted today has created hesitancy among consumers to send or receive private information unless encryption is applied, both during transit and at rest. Increasingly, banks or financial institutions not offering their banking customers a secure digital experience are regarded as disconnected and outdated.

Focus on customer experience as a digital business enabler.

Digitising and automating invoice processes are said to result in savings of 60-80 per cent compared to traditional paper-based processing. Some banks, including Standard Chartered, have set lofty goals to reduce their paper-based on-boarding from 90 per cent to 10 per cent by 2018. Standard Chartered is also expecting turnaround times to reduce from five days to less than an hour as a result of its investment in digitising processes. By encrypting on-boarding customer communications, including mobile, financial organisations can move towards these cost-saving models securely. And as a result, offer a cleaner, faster enhanced customer experience.

Invest in compliance and risk management.

The Cybercrime Directive and the recently-approved General Data Protection Regulation in the UK initiative have elevated the awareness of encryption technology. Under these rulings, banks and other financial institutions will be compelled to disclose when data security measures have been breached. They will also be required to justify the reasons for collecting specific customer data. Failure to comply, results in heavy financial penalties. Encryption has the ability to digitally protect sensitive data based on policies, minimizing the number one cause for data breaches, human error. Encrypting communications from the get-go is not only one way to avoid regulatory fines; it’s also an insurance policy for customers and business partners, building higher levels of trust.

This whitepaper sets out some of the key rules, guidelines, best practices and associated risks for FINRA member firms and suggests ways that organizations can use email technology to protect themselves, their customers and representatives. In addition, it looks at some of the other issues that enterprises may encounter when enabling the email encryption technologies.
Email communication introduces the risk of non-compliance with government and industry regulations along with substantial litigation and e-discovery costs.

The problem for regulated financial institutions is that inappropriate use of such widely available communications and collaboration tools can mean noncompliance resulting in hefty fines, potential loss of business, and fraud. In 2010, FINRA fined Piper Jaffray $700,000 for failure to retain approximately 4.3 million emails from November 2002 through December 2008. And in November 2009, FINRA levied a huge $1.2 million fine against MetLife for failing to establish an adequate supervisory system for the review of brokers’ email correspondence with the public. More recently, Societe Generale lost nearly €4.9 billion in fraudulent trades by a rogue employee that used insecure email and instant messaging communications to manage the transactions.

Virtually all company data is subject to discovery should legal action be taken, including communications traffic over emails and digital communications. In order to comply with most industry and government regulations, including FINRA, organizations need to demonstrate sufficient supervisory review; approval, security and retention policies and procedures are in place. However, in practice, not many firms are aware of the requirement or that there are solutions to meet the requirements. Virtually all company data is subject to discovery should legal action be taken, including all email communications and other types of electronic communications.

There are additional regulations outside of FINRA guidelines that relate to email and other forms of digital communications:

- **GRAMM-LEACH-BLILEY ACT (GLBA)**: Information protection, monitor for sensitive content and ensure not sent over public channels (e.g., Email).
- **SEC 17A-3 AND 17A-4**: Specifies the types of electronic records that must be preserved. Also specifies the manner and length of time that the records maintained by broker-dealers must be preserved.
- **PCI**: Ensuring cardholder data is not sent over unsecured channels and proving it has not occurred.
- **FEDERAL RULES OF CIVIL PROCEDURE (FRCP)**: Email and IM are ESI (Electronically Stored Information). Posts to social media sites must be preserved if reasonably determined to be discoverable.
- **SARBANES-OXLEY (SOX)**: Businesses must preserve information relevant to the company reporting. This means all email, IM and social media “conversations” are relevant.
- **CANADIAN SECURITIES ADMINISTRATORS NATIONAL INSTRUMENT 31-303 (CSA NI)**: Retain records for two years in a manner that allows “rapid recovery to a regulator.”
- **INVESTMENT DEALERS ASSOCIATION OF CANADA (IDA29.7)**: Requires the retention of records with respect to business activities, regardless of its medium of creation.
- **MODEL REQUIREMENTS FOR THE MANAGEMENT OF ELECTRONIC RECORDS (MOREQ)**: European requirements that define the functional requirements for the manner in which electronic records are transmitted and managed in an Electronic Records Management System.
THE CONSEQUENCES

Email was the dominant communication mechanism in 2015 with **over 116 billion business messages sent a day**. That's 116 billion chances for sensitive information to be intercepted – either with malicious intent or accidentally.

Due to technological advances and changes in the mobile workforce, portable mobile devices such as smart phones and tablets have made email usage even more prolific. The potential for data being compromised when using sending and receiving sensitive emails from all types of devices is much greater today.

A first step in implementing a plan for comprehensive email security is to understand the risks the organization faces. Over the years, there have been numerous examples of financial organizations losing data and reputeing as a result of an intercepted email. In 2013, LPL Financial was fined $7.5 million fine for email. To date, this violation is the largest ever brought by FINRA exclusively for email violations. It is just one more example of the regulator’s stepped-up enforcement effort to make sure emails are not being sent in the clear over public networks.

Furthermore, brokers and their firms will continue to be targets of disciplinary actions for failing to protect sensitive e-mails, especially where fast growth and increased regulatory requirements overtake stretched compliance resources.

All financial organizations must take a holistic view of their outbound email encryption requirements by viewing them as part of their overall security framework and infrastructure. Email encryption cannot be viewed as a standalone technology or activity, but as integral with an organization's control of data leakage and non-compliance.

A major part of this effort should be to identify who in a company has the greatest need for encryption and where the deployment of encryption would enable the creation of business processes not currently available to them. The groups that will most likely benefit most from encryption might include legal counsel, human resources, finance and other groups that regularly send sensitive or confidential information to others inside and outside the company.

**857.7 MILLION records have been breached since 2005.**

This is the equivalent to roughly 86 million records breached per year, that’s more than 230,000 records breached on a typical day, and about 187,000 records lost per breach incident.

That's alarming given the average cost of addressing a data breach tops $3.8 million US. The cost of a data breach varies by industry. The average global cost of a data breach per lost or stolen record is $154 US. As a final comparison, a data breach due to human error or negligence costs $137 US per record.

**1 Notification costs:** All necessary activities required to report the breach to appropriate personnel within a specified time period.

**1 Breach response costs:** All activities required to notify data subjects with a letter, telephone call, e-mail or general notice that personal information was lost or stolen.

**1 The cost of providing credit-monitoring services for at least a year.**

**1 Reputational damage.**

**1 Loss of business.**

**1 Negative publicity:** Extensive media coverage, further damaging the organization's reputation.
Protection of financial and personal customer information is a key responsibility and obligation of all FINRA member firms. Under the SEC’s Regulation S-P, firms are required to have technology, policies, and procedures addressing the protection of customer information and records. This includes protecting against any anticipated threats or hazards to the security or integrity of customer records and information and against unauthorized access to or use of customer records or information.

Firms should be aware that customer information and records could be compromised in a variety of ways. This is especially true for firms that offer online, web-based access to trading platforms and transmit customer account information over the Internet.

Firms must understand and address the potential risks of brokerage account intrusions, whereby an unauthorized person gains access to a customer account and either steals available assets or misuses the account to manipulate the market. Intrusions are generally accomplished through man in the middle attacks and the theft of the login credentials of a customer or firm employee.

Since this type of illicit activity can raise both investor protection and market integrity concerns, it is essential that firms use reasonable measures to protect customer information and assets.

FINRA protected information means any information, whether oral or recorded in any form or medium, that is created or received by a financial services organization; and relates to the customer’s financial transaction history.

Examples of FINRA Protected Information:

- ABA Routing #
- Bank Account Numbers
- Brokerage Terms
- Credit Card Numbers and Information
- Social Security Number Regular Expressions
- Trading Terms
- US Driver’s License (USDL) Details
- CUSIP Identification Numbers
- Employer Identification Numbers (EINs)
- Tax IDs

FINANCIAL SERVICES

Over 59% of financial services companies hold significant amounts of financial, health and personal information.

76.7% share the sensitive data they hold electronically with business associates.

FINRA
CEOs are very concerned about protecting company reputation and keep the company brand away from negative press. A data leak related to e-mail can severely impact how a company is perceived in the marketplace. The e-mail encryption of choice must protect company reputation and manage risks associated with data loss, internal governance, and regulatory compliance. A good CEO knows that damaged reputations can affect relationships with customers and clients, regulators and investors, as well as the ability to win new business, and attract and retain employees.

Can the sender easily send secure e-mail without any extra steps? Sending an e-mail is a behavior all of us do automatically; introducing encryption shouldn’t hinder this process. Likewise, the recipient should easily be able to open the encrypted e-mail. Good solutions will take these behaviors into account and keep them quick and efficient. Organizations can easily adopt encryption as long as their workflow doesn’t change.

Is the solution easy enough to integrate and manage across the organization? Can it adapt to your changing policy and regulatory requirements without impacting users? You can never predict where a security leak will come from. A cost effective solution will be adaptive and scalable to meet a wide spectrum of business requirements; protecting all secure information from going out in the clear, not just executives or specific departments. A cloud-based deployment model will also ensure the solution can keep up with the ever-changing security landscape.

Email encryption can be looked at as a corporate liability insurance. Companies may spend a lot of time and effort to protect their confidential data. However, they may miss prime opportunities to save costs and mitigate potential losses if they focus solely on protecting information, and ignore the benefits of a proactive e-mail encryption solution that continuously scans all outgoing mail traffic for keywords and regulation expressions in the body and attachments of the message. CEOs desire to wash their hands clean and utilize best security practices to enable data leak protection and liability indemnification.
Solving the Encryption Conundrum in Financial Services

PAIN POINTS - COMPLIANCE OFFICER

1. Regulatory Mandates
   - Is the solution going to help me comply with industry regulations? Will the solution comply with my best practices approach to running security? Is the encryption strong enough to prevent regulatory agencies from complaining about our approach? People often throw out the word encryption loosely. They assume their data is secure and encrypted; but often, the security profile has shortcomings. As these industry-wide regulations transform, so must your encryption approach. Organizations need to look at the type of encryption cloud-based service providers are using. Are they using the right encryption strength? If e-mail encryption is being used, is it adaptive to the regulations and the requirements of the senders and recipients? Given the evolving nature of state and federal data security regulations, the encryption solutions that coincide also must be evolving, adaptive, responsive, and interoperable.

2. Policies
   - Does the solution allow you to easily set scanning policies to inspect e-mail subject lines, body, attachments, and take action accordingly? You may only want to encrypt e-mails that contain certain keywords or regular expressions like credit card numbers or other customer information. A good solution will use a robust policy engine to allow you to create and edit policies to determine what should be encrypted and how.

3. Privacy & IP Protection
   - Data privacy is high on the security agenda these days; security has other important goals including protecting corporate data and intellectual property as well as controlling fraud. The value of the information or product that is lost has unprecedented consequences. When information is traveling over the public Internet via e-mail, compliance officers must take notice and deploy an e-mail encryption that contains the right combination of usability and security features.

4. Cloud Migration
   - As enterprises are increasingly adopting cloud-based solutions, shouldn’t your encryption decision follow the same strategy? Can the solution run entirely in the cloud, so you don’t have to run any software or hardware on premise? Cloud implementations save you deployment time and resources and allow the encryption solution to grow with the enterprise. Compliance officers need to ask a number of questions related to validity and security of a cloud email encryption solution but ultimately they recognize that only the cloud can help them scale and stay up-to-date without having to invest as security threats evolve continuously.

5. Cost Effectiveness
   - Is the solution easy enough to integrate and manage across the organization? Can it adapt to your changing policy and regulatory requirements without impacting users? You can never predict where a security leak will come from. A cost effective solution will be adaptive and scalable to meet a broad spectrum of business requirements; protecting all secure information from going out in the clear, not just executives or specific departments. A cloud-based deployment model will also ensure the solution can keep up with the ever-changing security landscape.
As encryption technologies improve in terms of efficiency, ease of use and interoperability, the risk of compromising client information is being reduced. Policy-based encrypted gateway services offer a viable and affordable alternative that allows entities to enforce email encryption behind the scenes without disrupting the day-to-day workflow of employees. One such platform is Echoworx’s OneWorld enterprise encryption platform.

OneWorld is a fully managed DLP (data loss prevention) encryption solution; administrators can define FINRA oriented policies around company confidential data that is being shared over the Internet.

OneWorld works as follows:
- All correspondence is scanned on the premises or in the cloud based on established FINRA policies.
- Built-in FINRA oriented dictionaries or lexicons search through each email (including attachments) to identify elements at risk, such as social security numbers, account numbers, account names etc and then automatically encrypt them when required.
- Any emails using that domain – whether via a smartphone, laptop or desktop system – are automatically scanned using the same policies.

The value this level of efficiency offers organizations is enormous. It not only relieves the burden of extensive training efforts, it also reduces the costs and complexities of managing encryption in-house.

IT managers can use a Web-based console to monitor what email is going out, the criticality and nature of the data and who is sending it; as well as set, review and customize privacy policies ensuring confidential content is automatically encrypted.

Automated encryption, based on defined business rules, will become an essential part of FINRA and other financial regulation compliance moving forward. A managed service model can speed deployment, ensure interoperability with existing systems and processes, and eliminate the risk of human error.

Echoworx’s OneWorld policy engine includes a number of pre-loaded FINRA and other financial industry oriented policies and regular expressions. A partial list is below:

- GLBA ABA Routing #
- Brokerage Terms
- Credit Card Information & Regular Expressions
- Social Security Numbers and their variations
- Trading Terms
- USDL (Driver’s License details)
- CUSIP Identification Numbers
- Employer Identification Numbers (EINs)
- Tax ID#
- Financial Terms & Dictionaries

Echoworx continues to update the policies as the FINRA, GLBA and other regulations evolve in the marketplace.
About us
Since 2000, Echoworx has been bringing simplicity and flexibility to encryption. Echoworx’s flagship solution, OneWorld Enterprise Encryption, provides an adaptive, fully flexible approach to encryption that ensures the privacy of sensitive messages. Enterprises investing in Echoworx’s OneWorld platform, are gaining an adaptive, fully flexible approach to encryption, creating seamless customer experiences and in turn earning their loyalty and trust.

For more information www.echoworx.com

✉ info@echoworx.com
📞 North America 1 800.346.4193 | UK 44 0.800.368.5334
🐦 @Echoworx