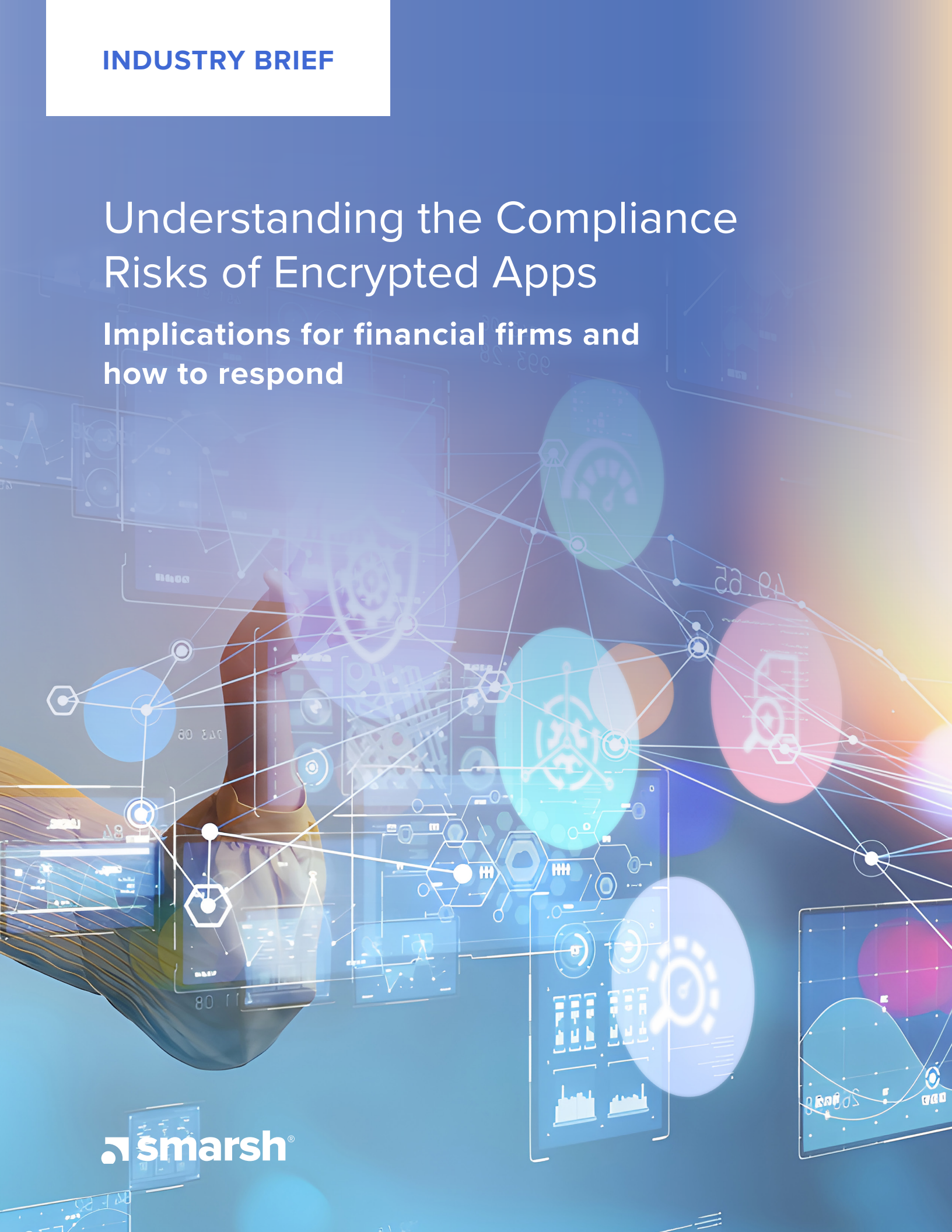
INDUSTRY BRIEF

Understanding the Compliance Risks of Encrypted Apps

Implications for financial firms and how to respond



marsh®

Introduction

Encrypted applications have become a popular way for finance professionals to communicate securely with each other and their clients. While encrypted applications like WhatsApp and WeChat are appealing and convenient, recent massive fines have made it clear that regulators are paying close attention to these new tools. Financial firms must take the necessary steps to ensure they are prepared to address regulatory compliance and other data privacy and security risks.

In a recent discussion, regulatory experts Robert Cruz, Shaun Hurst and Marianna Shafir explored how financial firms are using encrypted applications and what they're doing to address the compliance risks associated with these applications.

Featured Panelists

Robert Cruz
VP, Information Governance

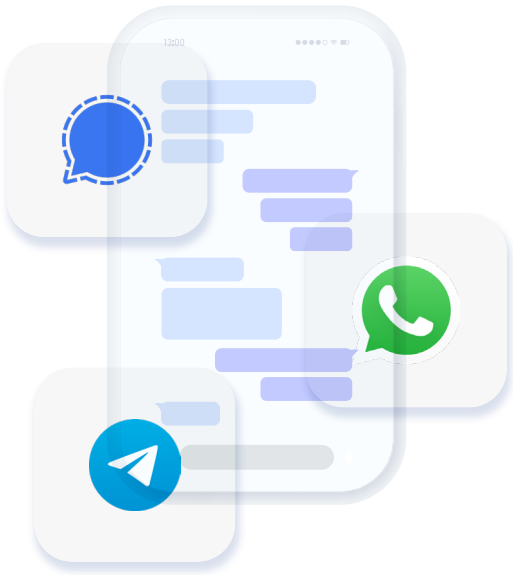
Shaun Hurst
Principal Regulatory Advisor

Marianna Shafir, Esq.
Regulatory Expert

What are encrypted applications?

Encrypted, or secure messaging apps, are mobile or desktop applications that provide end-to-end message encryption, so messages are only accessible to the sender and the intended recipient. Encrypted applications have become popular for both personal and business use.

In the financial services industry, encrypted applications are often used for client communication and employee collaboration. Popular encrypted applications like Signal, WhatsApp and Telegram are easy to use and offer various features such as voice and video calling, group chats, and file sharing. While these applications provide a higher level of security, they also make it more challenging for firms to ensure that business-related communications are captured and monitored in compliance with regulatory requirements.



"People are going to use these encrypted applications. There's nothing you can really do about that; it's part of our everyday life. It's probably become more prolific even since the whole lockdown phase during COVID. And the use of these applications increases the risk that communications might not be captured as they should, especially if you're giving financial advice."

– Shaun Hurst, Principal Regulatory Advisor, Smarsh

Regulatory Compliance Risks

With encrypted applications like WhatsApp now being used by over 2 billion users globally, it's more important than ever for firms to effectively manage the use of these apps to ensure they're protecting their organization from legal and compliance risks that can lead to fines and reputational damage.

Risks associated with encrypted applications include illegal or unethical activities such as sharing confidential information, coordinating unlawful activities, or spreading other harmful content. And while encrypted applications are designed to protect data from unauthorized access, they are not immune to the threat of cyberattacks, data breaches and other security risks that can lead to the loss of potentially sensitive information.

The use of encrypted applications poses several significant regulatory compliance risks for financial firms, including:

Failure to comply with recordkeeping obligations:
In the US, SEC 17a-4 and FINRA Rule 4511 outline data retention and accessibility requirements for business communications, including text messaging and other mobile communications. However, encrypted applications may not retain data in a way that's easily accessible or can be exported in an approved format, making it a challenge to respond promptly to regulatory inquiries or legal requests.

Failure to monitor and supervise communications:
Under FINRA Rule 3110, member firms are required to establish and maintain a reasonably designed system to supervise regulated employees, including reviewing all incoming and outgoing digital correspondence and internal communications related to securities business. To avoid non-compliance, firms should address encrypted applications in their WSPs, including what tools are allowed or prohibited, which individual(s) are responsible for monitoring and supervising the communications, how often reviews are conducted, and how they will be documented.

Failure to enforce WSPs:
Encrypted applications may also make identifying and addressing potential compliance risks more challenging. Many financial organizations have policies prohibiting these channels due to recordkeeping and supervision challenges. But that doesn't mean employees won't still use them. Suppose the organization has prohibition policies but no system for monitoring these channels to ensure representatives comply. In that case, the firm is still subject to regulatory enforcement and fines if the applications have been used for business purposes but not captured, retained and supervised.

"All firms here in the US are responsible for retaining records of digital communications that relate to their business. As per SEC Rule 17a-4, firms need to be aware of the requirements for monitoring and supervising electronic communications, environments review, and conduct, and capture for any misconduct. And it's critical that any size firm archives all business communications sent to and received by their reps."

– Marianna Shafir, Esq., Regulatory Expert

Firm size does not dictate risk

Large firms and organizations are not the only ones at risk when it comes to encrypted applications. Regulators are scrutinizing firms of all sizes. One significant penalty could cause harm to a firm from a reputational and financial perspective — big or small.

Staying ahead of risk

To mitigate these compliance risks, firms are taking several steps. Firstly, they are implementing strict policies and procedures regarding encrypted applications, such as guidelines on which applications are allowed, how they will be used, and who is authorized to use them. They are also training their employees on these policies to ensure they know what they are supposed to do and how to use encrypted applications safely and securely if allowed, as well as monitoring these channels to ensure compliance with company policies.

Implementing policies and procedures

When training, it's critical to obtain regular attestations from employees at the commencement of employment and regularly thereafter, such as annual attestations. Additionally, it's critical to outline which channels are permitted and which are prohibited on those attestations.

Why prohibition alone doesn't work

A common solution financial firms have employed to mitigate risk was prohibiting the use of encrypted applications altogether. However, prohibition alone does not work because people will still use these applications. It's not always down to the organization to dictate how employees communicate with clients. As clients and employee demographics change, these applications have become a part of our everyday lives.

The importance of training

Organizations must ensure that employees understand why they are doing what they're doing. Some larger financial firms have changed their approach to transparency in recent years, explaining to employees why certain training and rules are implemented.

"If staff understand why you're doing something, they're going to be a lot happier and more satisfied in their work environment. They'll also realize it's not just about using scare tactics and worrying about fines. There's a lot of value that can be had from enabling the use of these modalities."

– Shaun Hurst

A shift back to corporate-owned devices

Bring Your Own Device (BYOD) policies were once common at financial services firms. However, data privacy laws and regulatory rules such as SEC Rule 17a-3 and 17a-4, the Dodd-Frank Act, Sarbanes-Oxley, FINRA rules, MiFID II, CCPA and GDPR require regulated industries to securely archive business-related communications, regardless of what device is used.

A growing trend among regulated organizations is a shift back to corporate-owned devices to give organizations better control over employee communications. The inherent value of using an encrypted application like WhatsApp is that you can't have third-party integrations. Still, there's more control if organizations can control the mechanism employees use to communicate. From an EU perspective, it's the challenge between meeting regulatory requirements and your obligations from a data privacy perspective with laws such as GDPR.

Tracking down breadcrumbs of risk

Organizations must ensure prohibited channels are not being used for business communications, which requires frequent searching for breadcrumbs of risk. Firms can use lexicons and searches to monitor if their policies are working and what tools their reps are using. When firms are monitoring emails and electronic communications, they'll want to set up keywords for search, such as:

- "DM me"
- "Send to my Gmail"
- "Text me on WhatsApp"

In addition to traditional lexicon approaches, organizations are turning to AI and machine learning to help them surface risks and maintain compliance amidst the vast volume and variety of electronic communications data being generated today.

Any size firm must archive all business communications, whether sent to or received by their employees. This includes internal and external communications that are related to the business. With the sheer amount of data present and strict penalties piling up across the industry, the need to streamline and scale a more effective supervision review process has never been greater. AI-powered supervision and surveillance empower organizations to keep pace and future-proof their data strategy.

Conclusion

As technology advances and regulations evolve, organizations must keep up with both. Firms are focused on future-proofing their data strategies, turning to specialized solutions to help manage the risks associated with encrypted applications.

Today, communications channels are prolific, and organizations must account for their use with policies and enforcements and the right technology solution in place. It's not always about looking out for wrongdoings, such as insider trading or inappropriate outside business activities. It's about protecting your clients, yourself and your organization.

How Smarsh Can Help

Capture

Enterprise Capture: From email to collaboration to mobile devices and mobile apps, this module collects 100+ types of communications anywhere they happen to ensure you can support evolving business and compliance needs.

Enterprise **Archive**

This module applies intelligent retention policies to meet books and records regulations while cutting costs up to 50%. Data is stored in the Enterprise Warehouse so it can easily be used in surveillance workflows.

Enterprise **Conduct**

When you need broad, effective surveillance, the only answer is Conduct. Built on regulatory grade ML, the Conduct module scans any communications in the Enterprise Warehouse to surface up to 3x more real risk. Customizable scenarios increase the speed and effectiveness of reviewers by up to 3x over black box AI, even as data levels grow.

Discovery

Enterprise Discovery: Designed to support e-discovery requirements, the Discovery module lets you collect, review and place communications in legal hold in seconds. High speed, no cost exports ensure data is immediately available to counsel

smarsh®

Smarsh® enables companies to transform oversight into foresight by surfacing business-critical signals in more than 100 digital communications channels. Regulated organizations of all sizes rely upon the Smarsh portfolio of cloud-native digital communications capture, retention and oversight solutions to help them identify regulatory and reputational risks within their communications data before those risks become fines or headlines.

Smarsh serves a global client base spanning the top banks in North America, Europe and Asia, along with leading brokerage firms, insurers, and registered investment advisers and US state and local government agencies. To discover more about the future of communications capture, archiving and oversight, visit www.smarsh.com

Brief - 04/23

1-866-762-7741 www.smarsh.com @SmarshInc SmarshInc Company/smarsh