Moving from Reactive to Proactive Compliance Practices in Financial Services with AI

Co-created by **Emerj Artificial Intelligence** and **Smarsh**

emerj The AI Research and Advisory Company

smarsh

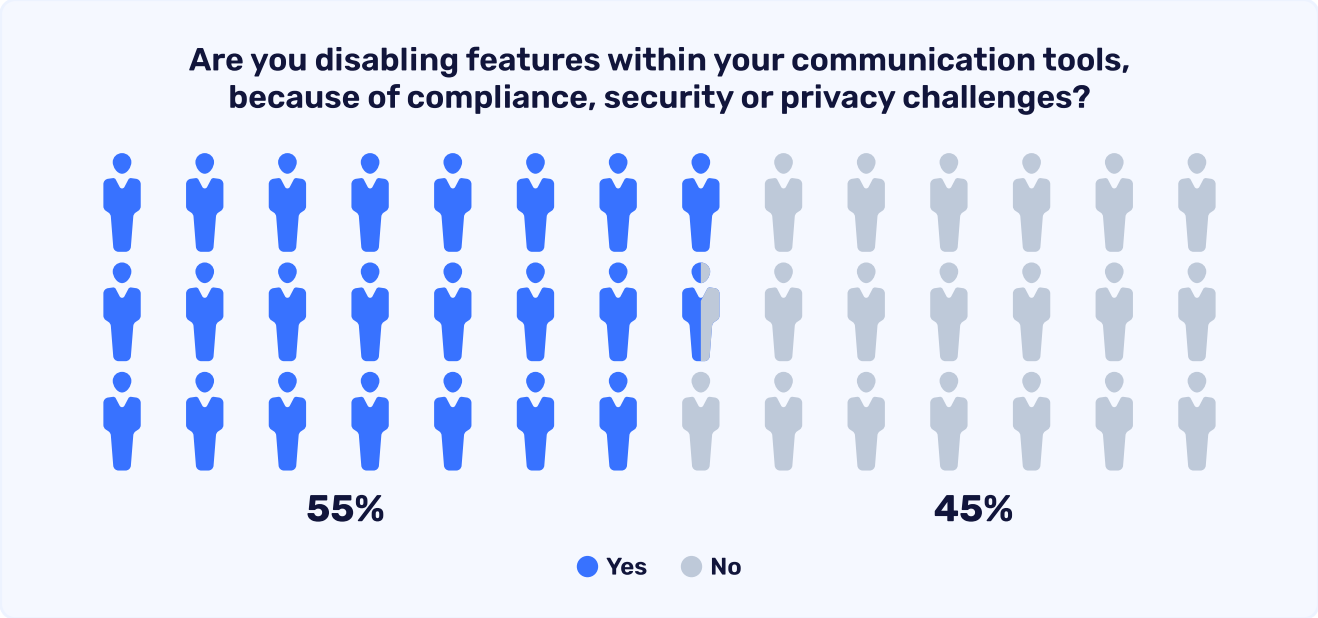
INTRODUCTION

In an era of rapidly evolving digital communication, the rise of novel platforms such as WhatsApp and TikTok has transformed the way individuals connect and share information. While these innovative platforms offer unprecedented avenues for communication, collaboration and customer engagement, they also present intricate challenges related to communications surveillance and regulatory compliance for financial institutions (FIs).

Amid this technological metamorphosis, regulatory frameworks originally conceived during the Great Depression era are struggling to keep pace with the rapid advancements of the Age of AI. In the process, these agencies are leveling serious fines against the largest financial institutions to show that these next generation communications platforms will be held to the same standards as any formal correspondence of the paper era.

In September of last year, the Commodities Futures Trading Commission (CFTC) and the SEC *leveled* over $2 billion in fines against a number of the biggest banks on Wall Street, including Bank of America, Goldman Sachs, Citigroup and Morgan Stanley. The year prior, JP Morgan alone *handed over* $200 million for not keeping sufficient records of unathorized messaging apps.

Meanwhile it appears financial institutions are woefully underprepared for the rising level of scrutiny. A 2022 *survey* from the security and compliance software firm Theta Lake cross verified by Thompson Reuters found that two thirds of the participating 500 compliance leaders believe employees at their firms are using unsupervised communications platforms.



Source: Internet World Stats - https://www.thomsonreuters.com/en-us/posts/investigation-fraud-and-risk/new-communications-demand-a-new-approach-to-compliance/

In leveraging new artificial intelligence tools in natural language processing and generative AI, financial institutions are finding effective tools for minimizing their exposure to a new generation of digital risk. In the process, a new standard is superseding how they've typically thought of these technologies in terms of increasing efficiency.

Far more important than efficiency, according to Smarsh Vice President of Information Governance Robert Cruz, is effectiveness. In more specific terms, Cruz gives concrete definitions for both:

"Where compliance leaders discuss efficiency, it means 'I want my people to make better decisions, faster and with more accurate results,'" Cruz tells Emerj. "The next step is effectiveness, which means that these leaders want to be sure that they have no risk exposure because they can see all the dark corners where potential violations can hide – and there are no surprises."

Robert Cruz
Smarsh Vice President of Information Governance

In this white paper, we will explore the multifaceted concerns of compliance leaders arising from the collision of new communications platforms and a regulatory regime racing to catch up with the times. In the process, we will provide comprehensive guidance on best data governance practices for achieving effectiveness over efficiency in their compliance operations.

We will explore these topics in the following subsections:

- Compliance Concerns Amid an Evolving Regulatory Regime
- Assessing Risk with Aging Tech Stacks, New Communications Tools and Updating Regulations
- Driving Effectiveness in Proactive Compliance Practices with Available AI Capabilities

COMPLIANCE CONCERNS AMID AN EVOLVING REGULATORY REGIME

The Broadening Surface Area

While many of the laws on financial record keeping date back to the 1930s and 1940s, they have been open ended enough to retain vitality through the age of fax machines, early cell phones and email without much adjustment. Through the better part of the last decade, there was a muted 'wait and see' approach to new social media platforms and communications tools expressed by regulators.

Following the fines lobbied against the biggest Wall Street banks last year, the message was clear, Cruz tells Emerj:

> *"The SEC is saying very clearly that it's all about preserving records that may be required to address a regulatory issue later – and it's not distinguishing voice video, whiteboards, email or social media. So the regulatory change and rules that are coming are looking at information agnostically. If it matters and it pertains to your business, it doesn't matter what the particular technology is that we're talking about."*
>
> 
>
> **Robert Cruz**
> Smarsh Vice President of Information Governance

In other words, the surface area for regulation – along with the price tag for not properly covering it – grew exponentially overnight for compliance professionals, leaving the entire industry on edge for when the next shoe will drop.

Arcangelo Grisi, Head of Market Surveillance for the U.S. at HSBC tells Emerj of the changing regulatory regime.

> *“There has been a push towards transparency, as markets are becoming more central in financial and communications ecosystems, transparency is becoming the rule. Much of the activity happens via electronic screens, so it’s all visible to everyone. Phone is riskier than screen, as transactions transitioning to screens may need new ways to analyze them. It is not necessarily easier to catch what happens on your phone.”*
>
> 
>
> **Arcangelo Grisi**
> Head of Market Surveillance for the U.S. at HSBC

Among the reason the surface area for regulation is so broad, particularly in the US, is that there are few ways for competitors in the banking industry to share information that's supported by current regulation, according to Kai Schrimpf, Global Head of Transaction Monitoring at HSBC.

> *"One of the things compliance officers have always pined for is more open data sharing between institutions, which obviously falls under regulatory and legislative scrutiny, but also internally: Why would we share data? Why would we share data with a competitor? While that is obviously a big hurdle, there are a couple of countries — specifically Holland and the Netherlands —who are at the forefront of getting all of their big banks to share data in a central repository by the government.”*
>
> 
>
> **Kai Schrimpf**
> Global Head of Transaction Monitoring at HSBC

The Generational Shift

That said, these platforms are not exactly new. WhatsApp has been around since 2009, so is there a larger catalyst for the SEC’s change in tune? Cruz can only think of one culprit:

> *“It's the fact that each generation of employee, each generation of client has its own preferences for the way that it chooses to interact. And what that means is that, you know, the tools that you are trying to control today are going to change tomorrow.”*
>
> 
>
> **Robert Cruz**
> Smarsh Vice President of Information Governance

In the view of regulators, newer entrants into the securities market space means a greater opportunity for fraud. In turn, the investor class is of an older generation and less familiar with the intricacies of these platforms. Just like your average high school students – younger financial professionals who came of age with TikTok and WhatsApp know where to go to avoid detection, even if they are mistaken.

ASSESSING RISK WITH LEGACY TECH STACKS, NEW COMMUNICATIONS TOOLS

Challenges Between Physical and Digital Communications

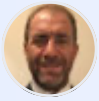
Making matters more complicated is where communications transcend from digital tools, both old and new, to physical media in the form of handwritten notes and whiteboard marks. That's before even getting into the fundamental intricacies of interpersonal communications in translating between different languages.

> *"If you talk to me on TikTok and you said, 'Hey, do you have time tomorrow?' That may be the only communication I'll be able to pick up, so I won't be able to decipher the meaning beyond the basic strings. That's what these models, in large part, are built to detect, but if it's in Spanish, when somebody doesn't speak English — or if it's emojis, or if it's a video recording, or if it's some other thing that's non-text — then your compliance efforts start to break down. When the SEC comes knocking on the door, the question becomes 'We know what they will ask about the use of prohibited communications tools, but don't know if what we've is good enough?' So that question of how do you traverse between these haystacks to find the needles that will get you into trouble? Nobody has the answer. It's not in a textbook. It's not in any regulator or federal guidance."*
>
> 
>
> **Robert Cruz**
> Smarsh Vice President of Information Governance

Perhaps the most significant problem underscoring these challenges, Cruz tells Emerj, is that everyone knows the regulators are coming, but there doesn't seem to be a playbook for how these penalties will be levied.

To get their hands around such a multifaceted problem, financial compliance leaders must understand the relationship between these different 'haystacks'.

Not only do they need to trace conversations and transactions between digital and physical realms, but they also need to navigate the disparate data streams from these platforms and the different 'languages' in which they communicate internally.

> *"Where we say, 'We've got all the answers for these questions but something just doesn't ring true. This guy says he works for a podcast company', but when we check, corporate database records, it turns out he's 100%, owner of a radio broadcasting company — the more effort it takes to reach that level of satisfaction, the less likely we are to say yes.*
>
> *Some institutions, particularly the newer financial institutions, the startups, et cetera, they're doing all of this in almost real-time by using very advanced algorithms. Search engines not only pick up the response that the client is giving but also pick up all sorts of factors around that response: How quickly did you respond? Where did you pause? Were you nervous? Did you have to go and when we asked you for your full name, did you have to go on? Can we hear you leafing through a document to find it?"*
>
> 
>
> **Nick Lewis**
> Managing Director of High Risk Client Unit, Conduct, Financial Crime & Compliance at Standard Chartered Bank

Road Maps vs. Heat Detection

In essence, the kind of detection systems that financial service leaders need to put in place to drive effectiveness over mere efficiency must be more akin to a road map as opposed to heat detection.

When deploying heat detection, a surveillance system can detect all the humans in a given area but they have no idea why they behave the way they do, neither where nor why they travel to different destinations. It knows where they are in relation to the sensor but knows nothing else about the environment in which they're operating.

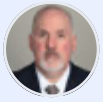
If armed with a roadmap, a surveillance system knows the relationship between different locations. If someone takes a trip to the grocery store, the system can draw far more specific conclusions about what they're trying to do and why.

It's this 'road map' level of insight that is necessary for financial leaders to effectively understand a potentially noncompliant transaction between a business plan written on a napkin and Lemoneight reservations.

DRIVING EFFECTIVENESS IN PROACTIVE COMPLIANCE PRACTICES WITH AVAILABLE AI CAPABILITIES

Having Clean Data from the Start

Many of the problems in understanding the relationships between communications platforms come down to the extant and fundamental challenges of big data.

> *"You have tons of data across your organization that you can't access, you have it buried in archives somewhere — and usually, none of this is updated: Someone in sales has more data, someone in credit risk has less and all of it's scattered. How can that all be pulled together? We need common operational methods and systems that can get these lines of business speaking the same language no matter how much or what kind of data they're using."*
>
> 
>
> **Thomas Mangine**
> BMO Director of AML & Risk Resilience

New artificial intelligence capabilities in natural language processing (NLP) and emerging generative AI tools like large language models pose tremendous benefits in helping large organizations better manage their tech stacks and data governance concerns across the enterprise.

According to Priyank Patel, SVP and Director of Financial Crimes Risk Surveillance at KeyBank, these new capabilities are making both anomaly detection workflows and the very practice of good data governance much easier than even just a few years ago.

> *"Holistically, the technology that most institutions had available until a few years ago made it all very difficult to monitor internal communications because you need infrastructure to process large amounts of data. Often, these systems were top-down in nature, which was prone to more false positives. Versus now, in the AI and machine learning space, it allows you to take a bottom-up approach, you can actually look at your data at a much more granular level, especially with the advancements in cloud computing, natural language processing and box libraries of keywords available in Python."*
>
> **Priyank Patel**
> SVP and Director of Financial Crimes Risk Surveillance at KeyBank

Cruz tells Emerj:

> *"Being able to draw connections between data repositories among these platforms effectively is a matter of good data governance practices; namely, having the cleanest data possible accrued from these channels from the start."*
>
> 
> **Robert Cruz**
> Smarsh Vice President of Information Governance

In order for these systems to properly interface with new AI data governance tools, they should feature:

- A proven, reliable and scalable method of capturing each model input from their original sources, where data privacy, securited and restricted content can be monitored.
- A method to account for differences across each source, such as voice, interactive elements or use of collaborative features.
- The agility to reflect changes in individual sources, such as the introduction of new features.
- Having data under management in a way that is already inspected for issues that might arise related to privacy, data security, restricted content or property like IP.

According to Marco Argenti, Chief Information Officer at Goldman Sachs, generative AI can have a huge role in engineering systems so that organizations can minimize insider risk through controlling the flow of information through the organization.

> *"If you think about AI and especially generative AI, as the next evolution of a technology that has been around for decades, among the first imperatives for us is to try to be very prescriptive with regards to how our employees and how our developers are using AI to allow us to really implement AI training and AI inference for a number of use cases like analytics, anti-money laundering or surveillance.*
>
> *And we can apply the same approach - which is an approach where you put safety and accuracy first - you can also try to remove some of the sharp edges that could potentially be there by really tightly controlling. That's what we call the 'control plane,' or basically the way people access information, and what kind of entitlements they have to information."*
>
> 
>
> **Marco Argenti**
> Chief Information Officer at Goldman Sachs

Off-Channel Communications

Advanced analytical approaches are particularly effective when potentially noncompliant activity is detected on an off-channel line of communication, such as a YouTube or other prohibited network or where communications leading to a potentially fraudulent transaction suddenly drop off in an official communications stream.

Usually, such activities trigger an investigation where, Cruz tells Emerj, NLP AI and large language models will be instrumental in tracing the remainder of the conversation on other suspected platforms. For instance, if compliance leaders find an employee and a client talking about an IPO, and in that context they see a suspicious word – that might be in code – appear again and again in communications.

Because of different regulatory obligations and personal data privacy concerns, there is always a balance to maintain between personal and business communications. Yet with extended context and powerful language search tools at their disposal, compliance professionals can use available and universally approved tools for that first level of inspection to determine if there's a larger area of risk exposure they need to be tuned into.

ABOUT SMARSH

Smarsh was founded in 2001 by Stephen Marsh. A veteran of the financial services industry, Stephen recognized that traditional regulatory retention and oversight requirements applied to new and emerging communications technology. Smarsh has grown significantly over the past 20 years.

Our solutions have evolved to ensure that we can tackle the constantly shifting compliance challenges facing our more than 6,500 clients; from small businesses to multi-national banks. We have over 1,400 employees worldwide. Collectively, we have unrivalled expertise in implementing SaaS solutions and a deep understanding of the regulatory and compliance issues impacting modern businesses.

smarsh

Visit
smarsh.com

Contact
smarsh.com/sales-contact

ABOUT EMERJ AI RESEARCH

Emerj Artificial Intelligence Research is a market research and advisory company focused exclusively on the business impact of AI.

Companies that thrive in AI disruption run on more than just ideas. They leverage data and research on the AI applications delivering returns in their industry today and the AI capabilities that unlock true competitive advantage into the future - and that's the focus of Emerj's research services.

Leaders in finance, government, and global industries trust Emerj to cut through the artificial intelligence hype, leverage proven best-practices, and make data-backed decisions about mission-critical priorities.

emerj
The AI Research and Advisory Company

Visit
emerj.com

Contact
research@emerj.com