

Banking on the Future of AI-Driven Compliance with Experts from UBS, HSBC, BMO and More

Co-created by

Emerj Artificial Intelligence and Smarsh



As of 2022, AI's collision course with the financial service sector is well underway. What began with a mass migration to digitization and AI in the initial shock of the COVID-19 pandemic is here to stay – and growing stronger in the pandemic's wake.

Financial services enterprises, in particular, are increasingly turning to AI capabilities to manage increased regulatory burdens and improve risk management amidst "limited organic growth, volatile capital market returns, and fee and margin compression," according to a recent assessment from Deloitte.

Among the changes is a compliance perimeter that "now covers new areas such as board governance and third-party risk management, along with detailed requirements in prudential risk management such as capital and liquidity management," as summarized in the introduction of another recent Deloitte report on the outlook for banking regulations in 2022.

As in just about any modern-day technological arms race, AI is an essential tool in the arsenal for financial institutions (FIs) of every stripe.

On the AI in Business podcast, we regularly hear from financial leaders and compliance professionals worldwide about these various challenges. Among their most actionable advice is that which focuses on adopting AI capabilities in search of new and easier ways to scale operations in insider risk detection for increasingly complex contexts.

This whitepaper will examine three distinct use cases in compliance for large-scale financial enterprises described by our podcast guests across the banking and financial services industries. These examples demonstrate the broad application of AI technologies in the compliance space for FIs and what they mean for the future of the sectors therein:

→ **Infusing legacy systems with intelligence**

Using data analytics and machine learning to reduce time spent verifying false positives and leverage the massive data trove from the convergence of legal and regulatory requirements.

→ **Communications surveillance for financial market misconduct**

Using natural language processing (NLP) to detect malicious trader behavior in written or spoken communications faster.

→ **Market surveillance beyond typical language-based communications**

Obtaining a 360 view of employee activity in the context of compliance and the realities of the larger market by going beyond the literal meaning of communications being collected through traditional means.

Much of our sourcing for these use case descriptions come directly from feedback from our expert guests shared on their respective episodes of the AI in Business podcasts. We will, however, incorporate outside sources to corroborate and contextualize their testimonies.

We will begin by examining how communications surveillance of audio and text-based conversations are used to disclose financial criminality and insider risk.

Making Legacy Systems More Intelligent

Few organizations are better familiar with the challenges of legacy systems than the Bank of Montreal – an institution that predates Canadian independence by almost half a century. These challenges can [include](#) the following:

- ❶ Maintenance costs
- ❷ Security loopholes
- ❸ Constant updates and patchwork fixes
- ❹ Unstructured data that cannot be updated

Director of AML and Risk Reliance for the Bank of Montreal Thomas Manginge described at length what every organization should do to address these challenges on a recent [episode](#) of the AI in Business podcast.

In working with legacy systems in the form of on-premises software, Manginge tells Emerj that American FIs especially will need to focus on drawing data out of their archives to compensate for the increased traffic of larger AML, cybersecurity, and compliance teams being in the pipeline.

Making sure the IT team is on board with handling the increased traffic, leadership is clearly communicating their needs, and that infrastructural demands are met ahead of that traffic are all essential, Manginge tells Emerj. In many cases, budgetary and workforce concerns mean these changes will need to be phased over time and usually require an interim solution to handle short-term problems.

Respecting the subject matter expertise of IT and cybersecurity professionals in particular – rather than expecting them to meet idealistic expectations uninformed by technical context – will mean valuable feedback and maximum value for time spent:

“ *If you come to an engineer, and you tell him specifics of what you want, you will get very focused questions based on getting greater resolution, and he will tell you [not only] what he can do and what he can't do but [also] what he might be able to suggest, based on what you've said you want it and he can't do...*”

Thomas Manginge, Director of AML and Risk Reliance for the Bank of Montreal

“ *If you come in and say, 'Well, I want to be able to access more data in a very generic manner,' then you're going to burn a lot of time, and you're going to probably burn a lot of patience. As you guys go back and forth with a 'Well, I need you to explain to me more of what you want.' Starting those conversations upfront is critical.*

Thomas Mangine, Director of AML and Risk Reliance for the Bank of Montreal

It's often in conversations between business and IT leaders that carefully considered AI solutions – from outside vendors or the seeds of early in-house digitization projects – can be sewn to make the most significant difference in bringing legacy systems to the 21st century.

Among AI capabilities in the current tech landscape, machine learning and data analytics-based solutions stand the best chance of overcoming legacy system challenges, particularly in addressing problems in workflows and the high volume of false signals.

However, a poignant challenge for legacy banks in integrating third-party systems and vendors is that outside influences can throw a wrench in the initial phase of addressing IT and internal security team concerns.

According to Thomas Mangine, the best way to address the conflict of interests therein is for business leaders to make cooperation between vendors and IT teams their top priority. Yet most of all, leaders must ensure internal teams' concerns in tailoring the overall approach to the specific challenges of their legacy systems supersedes vendor ambitions.



Actionable Takeaways

The first and most crucial step is ***coordinating an introductory meeting with IT, information security, and/or cybersecurity teams within the organization*** about:

- Where data is stored.
- What data is available for ready access.
- What infrastructure is needed to create increased accessibility of old data and security for new data.

For on-premises software solutions, IT teams must be:

- On board with handling the increased traffic.
- Leadership is clearly communicating their needs to the rest of the team.
- And infrastructural demands are met ahead of that traffic.

In working with outside vendors/SaaS products:

- Business leaders must make cooperation between vendors and IT teams their top priority.
- The concerns of internal/IT teams in tailoring the solution to specific challenges must supersede vendor ambitions.

If budgetary or workforce concerns are an issue, leaders must devise a long-term strategy for solving the problem with an interim solution that covers short-term concerns.

There are three primary features of a system designed to best negate false positives:

- A keen understanding of human behavior off-line and their ability to consciously work around evolving rules-based systems.
- How humans act before and after misconduct in online or surveillance environments.
- How these patterns typically appear regarding traceable misconduct in market surveillance.

Detecting Market Misconduct Risks Through Communications Surveillance

Historically, there have been two primary drivers for enterprises looking for value in AI to address compliance challenges in the financial space: **legal** and **regulatory**.

In terms of regulation, financial services firms are required by regulators around the world to do the following in the name of keeping markets and their organizations free from criminality:

- To gather and consolidate their communications data.
- Store and archive that data according to rigorous protocols.
- Then analyze that data in search of misconduct.

Simultaneously, the risk of litigation and other legal exposure forces firms to put communications on a legal hold as they conduct internal investigations.

These dual obligations working in tandem over the last three decades bring us to the situation today where companies are stockpiling massive troves of legacy (i.e., letters, paper documents) and digital age communications data (i.e., emails, cell phone calls, online transcripts, etc.).

In the past and up through the age of email communications twenty years ago, compliance professionals were reduced to engaging in time-consuming ad hoc searches, trying to find proverbial needles in tall haystacks.

As communications volumes have increased with new technological advances and communications mediums (**including a 50 - 100 % increase in volumes in the post-pandemic era, according to Brandon Carl**) – the amount of communications to survey is too much for humans to accomplish on their own.

Adding to the array of challenges is the rarity of actual insider misconduct, which is often infinitesimally more infrequent than incidents of fraud – a behavior that is also quite infamous in the compliance field for producing false signals in detection methods.

The traditional workflow for detecting insider risk includes the following:

- 1 Compliance professionals begin with what's called a [lexical approach](#), involving keyword searching through communications for terms indicative of misconduct ("fixing LIBOR" or "pumping," as examples).

- 2 These keywords would generate a comprehensive volume of alerts, most of which are false positives.
- 3 Compliance professionals then assess a portion of these alerts most likely indicative of criminal behavior, deciding which are relevant or not with human judgment.
- 4 If an incident that triggered an alert is decided to be relevant, they enter an escalation workflow to judge whether to proceed with an investigation.

Given the repetitive workflows traditionally involved in compliance surveillance and how they can exacerbate many of these problems, the space is particularly ripe for automation and AI solutions to help streamline the process.

In Brandon Carl’s experience, machine learning-based solutions appear particularly well suited for streamlining compliance workflows in finance among the range of AI capabilities currently available.

“The key invention with [machine learning] technologies has been the ability to really improve the signal-to-noise ratio, to filter out a lot of the noise, and to actually focus in on finding new forms and new types of misconduct,” Brandon tells Emerj.

These solutions make a world of difference in the banking compliance space that requires daily review of communications alerts. Too many false positives alert slow review teams and prevent them from doing their best work:

“ *Historically, when reviewers would go through alerts, you can imagine almost an Orwellian world where 99 out of 100, or 999, out of 1,000 of these alerts would actually be irrelevant. And so there have been people whose job was effectively the majority of the day just to click “irrelevant”. That we’ve been able to do with some of these AI technologies is actually filter out so much noise that they have a lot more signal they can focus in on.*

Brandon Carl, EVP of Product Management at Smarsh


Actionable Takeaways

Given the multifaceted nature of present challenges, banks and FIs should be looking for efficient, comprehensive solutions in communications surveillance that can:


- Improve program worker and cost efficiency.
- Broaden risk coverage and increase risk detections.
- Increase compliance agility and insights.

To streamline communications surveillance workflows, leaders should look for AI-powered banking compliance solutions that allow compliance teams to:

- Filter out the evident noise.
- Find the specific language of interest that may be concerning.
- Have certainty that behavior is happening in a specific context of misconduct ahead of a possible investigation.

 **Mitigated Risk**

- **500%+** risks identified
- Up to **95%** false positive reduction
- **300%** true positive increase

 **Improved Return on Investment**

- Supervised users with **25%** less staff
- Reduced discovery volumes by **40%**
- Produced TCO savings of **64%** over 3 years

AI-driven compliance risk-detection efficiency reported by Smarsh clients. (Source: Smarsh)

Other advantages of AI-enhanced banking compliance solutions include helping compliance professionals:

- Stay better prepared to handle surges in the volume of communications data.
- Lay the groundwork for investigations in addressing bias and fairness.
- Adjust to new communications channels and expand regulatory surfaces.

Market Surveillance Beyond Typical Language-Based Communications

As regulations expand with technological advances, compliance expectations and "regulatory surfaces" are expanding far past text- and audio-based digital communications.

Market and trade surveillance in these contexts generally includes both e-communications and that behavior taking place outside the contexts of individual FIs and their communications channels. Specifically, the term tends to frame events in the greater realms of competitors, the larger markets, and the everyday life of financial professionals not taking place on their company-registered chat and texting apps.

With the expansion in regulatory surface, our expert guests tell Emerj that these more extensive areas of market and trade surveillance are becoming an increasingly higher priority for legacy banks and a fertile terrain for early AI applications at these organizations.

Among them, Head of Market Surveillance for the U.S. at HSBC Arcangelo Grisi [attests](#) to the impact of present trends in supply and demand:

“ There is one interesting thing that is happening to market surveillance. It's that, beyond the typical market abuse detection that we just mentioned – right before insider trading, spoofing and front running beyond the typical inner market – that is detection. There are actually AIs that are built around trading behavior. Imagine that these AIs will just look for outliers in your trading behavior, or they will look for an outlier in the trade life cycle and will flag an alert. And then the analyst, of course, will need to look at this in conjunction with everything else and to make a determination.

Arcangelo Grisi, Head of Market Surveillance for the U.S. at HSBC

The ever-increasing demand for enough trade surveillance context is a problem keenly felt by compliance teams for legacy FIs. Thomas Mangine tells Emerj that is because regulatory expectations for compliance go much further than the surface information banks have on their clients and reach know-your-customer levels of complexity.

Market and trade surveillance also entail the complicated and somewhat awkward requirement of sharing information with competitors – a situation discussed at length by Global Head of Transaction Monitoring at UBS Kai Schrimpf in his appearance on the AI in Business podcast.

Actionable Takeaways

The inevitable solution for banking leaders is moving their organizations from rules-based to risk-based systems.

Rules-based systems are:

- Continually subject to the cat-and-mouse arms race between financial criminals and authorities.
- Inherently reinforce a status quo of playing catch-up that gives financial criminals the advantage of being assumed to be ahead of banks and law enforcement.

On the other hand, risk-based compliance systems are:

- Better at recognizing that inherent lack of stasis in the very nature of the kind of misconduct they're trying to find and ultimately prevent.
- Leverage the capability of AI tools like machine learning to trace deeper patterns in human behavior that go beyond constantly evading existing rules.

Our expert guests attest that the AI tools in market and trade surveillance best suited for helping organizations transition from rules- to risk-based systems:

- Involve some degree of data analytics and machine learning.
- Must be constantly fed new and unique forms of data to help these tools draw conclusions outside routine communications surveillance.

About Smash:

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 advisors and U.S. state and local government agencies. To discover more about the future of communications capture, archiving and oversight, visit www.smarsh.com.



Visit:

www.smarsh.com

Contact:

smarsh.com/contact

About Emerj Artificial Intelligence 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 return 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.



Visit:

www.emerj.com

Contact:

research@emerj.com