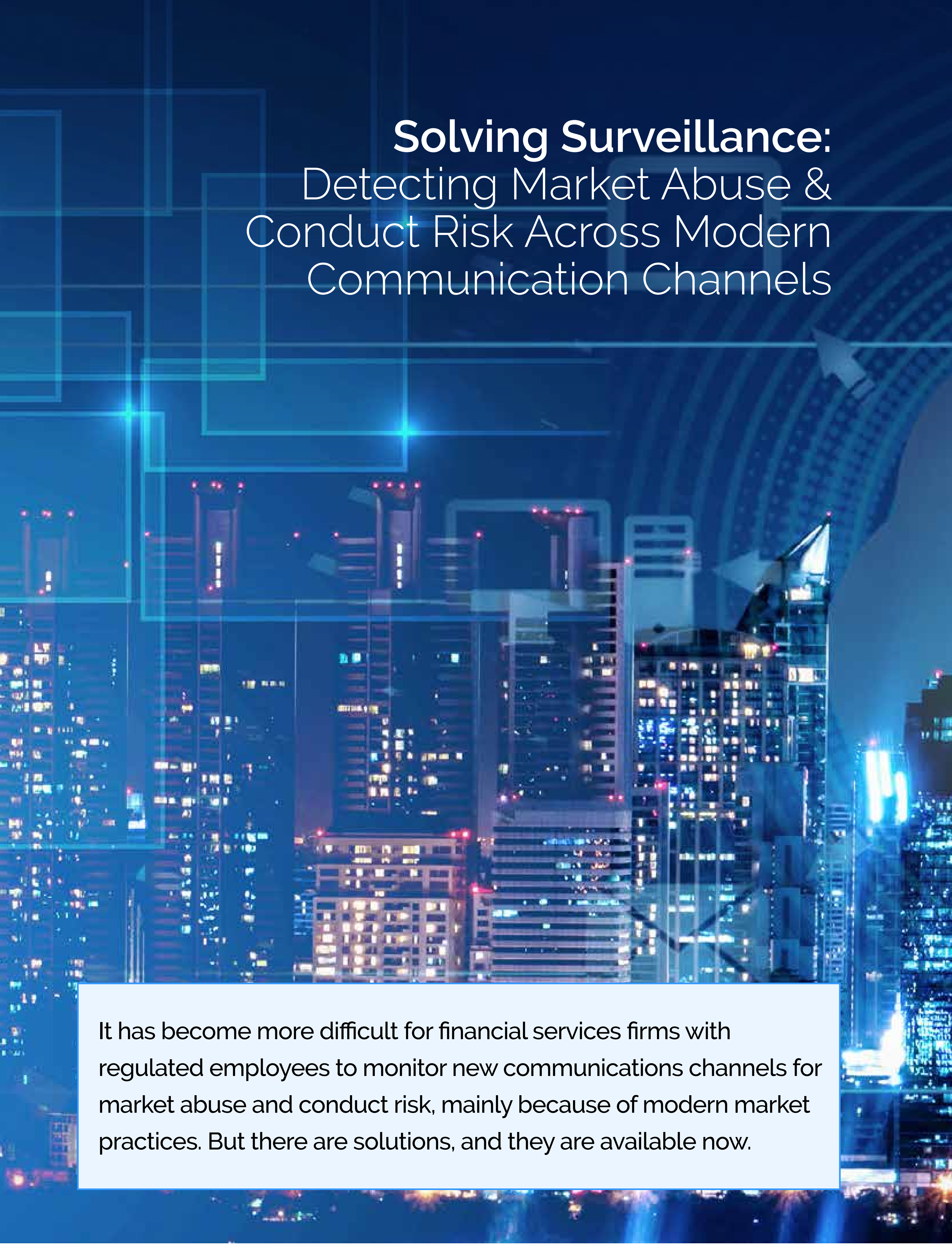
A 1LoD publication

in-Focus Report®

Commissioned by: NICE Actimize

Solving Surveillance:

Detecting Market Abuse & Conduct Risk Across Modern Communication Channels



Solving Surveillance: Detecting Market Abuse & Conduct Risk Across Modern Communication Channels

It has become more difficult for financial services firms with regulated employees to monitor new communications channels for market abuse and conduct risk, mainly because of modern market practices. But there are solutions, and they are available now.

> *Banks must now consider whether they are in compliance across every communication channel where their regulated employees communicate,*

In the past 10 months alone, 12 major financial services institutions have been fined a total of $2 billion for failing to keep records and monitor staff adequately. This should be a game-changer for those working in the 3 lines of defence and their senior managers. The fines exceed punishments for similar lapses in the past, much to the surprise of the banks which admitted publicly that they had not expected this level of enforcement.

Regulators are concerned that more and more conversations between regulated employees and their clients occur across a range of channels which lie outside the regulators' reach, hampering their ability to conduct investigations. In one instance, the SEC said that a bank failed to search employees' personal devices, and that its "record-keeping failures impacted the commission's ability to carry out its regulatory functions".

Banks must now consider whether they are in compliance across every communication channel where their regulated employees communicate, including unified communications platforms (such as Teams, Zoom and Cisco Webex), IPC Unigy or other turrets, Cloud9, mobile phones or PBX (desktop phones). They admit that employees have used these channels to communicate in ways that circumvent legal record-keeping requirements, but they also question whether it is realistic to comply with rules which are at odds with the ways in which banks and their clients do business today.

Is that worry justified?

Time for change

The concern is only justified if banks continue to rely on outdated capture, archive and analytics platforms. Many banks still use point surveillance systems to record and monitor different communication channels. Aggregating these separate data feeds is difficult and leads to issues with surveillance, case management and investigations. Maintaining these stacks, for example by patching, and establishing centralised governance and assurance over them, is also difficult.

Too many processes are still done manually or inefficiently. This is a poor use of resources which could be deployed more effectively in compliance and surveillance tasks with a higher added value. In the case of new messaging channels such as WhatsApp, banks can spend months creating a solution for that one particular channel, but then when communications migrate to a new channel (which happens frequently), the banks have to go through the process all over again. In the case of collaboration tools such as Zoom and Teams, again, the banks need separate solutions for the tool and even for different embedded functionalities within the tool.

Surveillance professionals know this, of course, and many want to move to more efficient solutions, but they are hampered by complex budget and organisational considerations. Only a handful of the very largest banks can afford to build in-house, or to maintain large and complex solutions stacks, or to deal with the integrations required on the premises. The answer is simple: financial services firms need a one-stop solution which can provide all of the functionality they require out of the box and in the cloud.

> *Using advanced analytics and AI (including Natural Language Understanding), Compliancentral can accurately detect all types of market abuse and conduct risk by monitoring the communications of regulated employees across every type of channel.*

Moving to a single vendor

To meet regulators' requirements, firms need a compliance recording and monitoring solution that is able to solve both parts of the problem. First, firms need a capture, recording and archiving solution that records and retains communications across the many channels where regulated users communicate, while being flexible enough to allow firms to stick to local capture and storage requirements. Second, firms need a surveillance solution that can take the captured data, analyse it effectively against defined market abuse and conduct scenarios, and generate accurate alerts. Ideally, a solution would incorporate the latest new technologies in terms of automation, machine learning (ML) and artificial intelligence (AI) while being able to incorporate existing lexicon-based analytics, existing scenarios, rules, and calibrations. It would be even better if both needs could be met with one solution.

This type of solution would offer a consolidated, centralised approach to managing recordings and provide a central vantage point for tracking all global regulated users and communications. It would not only reduce regulatory risk, but also reduce costs and make patching and updating simpler. And it would, almost as a by-product of meeting these other requirements, lead to faster and more accurate trade reconstruction and investigations.

The claims made by technology vendors often sound confusingly similar to their bank customers, and are hard to evaluate. Plus it is hard for banks to change their current processes. However, the recent high-profile enforcement actions show that the current situation is untenable and that it is time to change.

Modern, integrated solutions allow banks to look holistically at their data in real time and detect misconduct while freeing up resources to focus on value-added activities. They also allow banks to start thinking about problems before they occur – rather than discovering them after the fact – by monitoring broader sets of behaviours over larger populations in order to look at culture and misconduct proactively.

Today's technology

NICE's end-to-end Communication & Trade Compliance suite, Compliancentral, brings together NTR-X to provide communications recording and archiving, and SURVEIL-X, the industry's leading holistic conduct surveillance and behavioural insights solution, into a single cloud-based compliance platform.

Using advanced analytics and AI (including Natural Language Understanding), Compliancentral can accurately detect all types of market abuse and conduct risk by monitoring the communications of regulated employees across every type of channel – turrets, desktop phones, mobile, email, instant messaging, chat, texts, social media, unified communications and even document attachments. Compliancentral also uncovers hidden conduct risks by correlating employees' actions (trades and behavioural data) with their communications patterns and activities by merging trade, communications, and behavioural data into a single case management solution for more accurate and effective conduct risk monitoring and investigation. If regulated employees try to get around monitored communication channels by switching to "offline" conversations, the system can help detect this behaviour.

Compliancentral is revolutionising the way that financial firms comply with global regulations and identify conduct-related risks by correlating employee actions (trades and behavioural data) with their communications. This can help banks to understand what their employees said, heard and did, so that they can uncover hidden risk more accurately and efficiently.

In Summary

Trust lies at the heart of financial compliance. It is crucial for any bank's reputation, for its bottom line, and for the integrity of the broader market. But as every bank knows, risk can hide anywhere – in the millions of daily calls, emails and instant messages, in the exciting new communication channels used for hybrid work, and in the growing trade volumes.

Detecting risk in this ocean of data is extremely difficult, but this is precisely where Compliancentral can help, shining a light on misconduct and exposing risk before the damage is done.

Learn more by visiting www.niceactimize.com/compliance