A 1LoD publication

in-Focus® Report

Commissioned by: Relativity®

Surveillance in a post-COVID world

July 2020

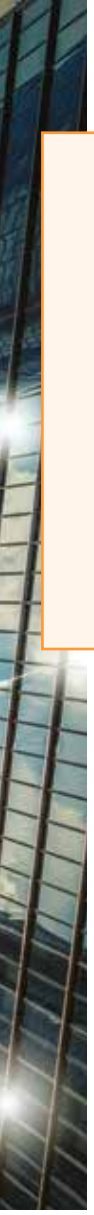
» Surveillance in a post-COVID world

COVID-19 triggered a sea change in the banking functions charged with ensuring that conduct and regulatory compliance remain robust. This in-Focus Report sets out the challenges surveillance faces in both a locked down and post-pandemic world, and the tech and work practices that could help them meet the new normal head on.

When the coronavirus pandemic forced the world into lockdown in March 2020, it also sent shock waves through financial markets. That initial storm – during which banks shouldered the gargantuan task of enabling thousands of traders, sales people and other risk takers to work from home, and market volatility swamped surveillance teams with a surge of alerts – has now passed. But it has provided a wake-up call for banks' compliance heads, laying bare a string of pre-existing weaknesses or inefficiencies in the function, and tossing up major new risks for them to monitor and mitigate.

As the dust settles and remote working becomes the new norm, risk takers have migrated to an expanded and previously untested suite of communication channels while also being less visible to their supervisors. This has given banks' surveillance teams a hugely complex set of challenges. At the same time, scattered surveillance team members have a need for more intuitive collaboration and case management tools, as well as smarter rules to limit any future spike in alerts. Banks are also required to develop innovative workarounds and make targeted tech investments.

"The world is changing but you have the same responsibilities," notes Jordan Domash, General Manager of Relativity Trace, a communication surveillance application built on the Relativity platform. "To adapt, you need technology that can ingest communications from new channels. Also important are configurable workflows that enable practitioners to conduct their entire process in a defensible way within the tool, without leaving it to conduct escalations in an untracked way over email, SharePoint or Zoom."



Initial fire fighting

In the early weeks of lockdown, banks' compliance functions entered fire drill mode, scrambling to maintain 360-degree surveillance coverage as traders, salespeople and their own team members were relocated en masse.

Operational resiliency was tested at a basic level, with banks rushing to supply staff with the screens, phones and internet connectivity they needed to work remotely, while communication and collaboration platforms like Zoom, Slack or Microsoft Teams were signed off and implemented at speed.

Compliance practitioners interviewed for this in-Focus Report said that despite some teething problems – for example, faulty turrets or incompatible phone recording systems at business continuity back-up sites, plus the discovery that a surprising number of senior bankers had no internet at home – the process was relatively smooth.

"One challenge that refuses to go away, however, relates to banks' ability to capture risks completely in a world where traders and other risk takers are working outside a controlled office environment – and may continue doing so for some time."

A tidal wave of alerts

Far more challenging for compliance teams was an influx of trade and communication surveillance alerts – for some business lines reportedly 1,000% higher than typical daily volumes – warning of potential market abuse or collusion. This was triggered by a surge in both market volatility and unusual behaviour, as traders and salespeople, through necessity rather than ill intent, made heavy use of email and mobile phones – up 300% at one bank – while recording equipment registered an uptick in red-flag lexicons, including typically benign promises to call colleagues at home or via unauthorised channels such as WhatsApp or Zoom.

Compliance practitioners interviewed for this in-Focus Report said despite the challenges some faced using manual, lexicon-based tools, they were ultimately able to close out all the alerts that came their way, albeit with temporary backlogs. One, however, said peers at other institutions had admitted they were forced to review only their highest-priority alerts. A second practitioner regretted his bank had not invested more in AI solutions that would have weeded out false positives and made such prioritisation more possible.

One said his bank had made a conscious decision not to adjust thresholds significantly in an effort to reduce alert generation and that this was the right decision, but another reported that the early pandemic weeks had persuaded him of the potential benefit of investing in technology that automatically redefines thresholds in response to changes in market volatility.

A learning experience?

The risk of market abuse occurring was also genuinely higher, with governments' quantitative easing and bond buyback activities, for example, creating opportunities for manipulation that banks' surveillance teams needed to create new controls around; all this at a time when the function was already under strain.

In retrospect, the first weeks following lockdown were "a good learning experience" for the surveillance industry, the head of trade surveillance at a European bank told 1LoD. They "highlighted how flexible we were in certain areas and how inflexible in others."

A couple of months in, market volatility has eased significantly, compliance teams are no longer swimming in alerts, and banks' trading and surveillance functions are settling fairly well into new ways of working.

One challenge that refuses to go away, however, relates to banks' ability to capture risks completely in a world where traders and other risk takers are working outside a controlled office environment – and may continue doing so for some time, noted Alan Lovell, global head of surveillance at HSBC and one of several practitioners interviewed for the report.

Surveillance black spots

Voice and e-comms are the biggest headache for surveillance teams in terms of data capture. At a recent 1LoD Digital Debate, nearly 65% of attendees said their bank was currently undertaking a review of its supervisory controls in response to the COVID crisis, and interviewees confirmed this is certainly true in the case of comms. It remains a work in progress, however, as banks experiment with a combination of tech solutions and practical workarounds.

In a regular office-based world, staff are required to direct all business communication through a limited number of approved channels, such as a desk phone, work mobile or business email account. On a trading floor, verbal conversations between team members are also often captured via on-desk turrets. These rules help ensure that work-related communication can be captured in its entirety in a specified format that is compatible with the bank's existing analysis tools and other tech. Policies surrounding this – for example, prohibiting the use of personal mobile phones on the trading floor – can also be easily enforced when risk takers are surrounded by and visible to their colleagues and Supervisors.

And while traders seeking, for example, to engage in collusion can theoretically leave the building to meet their collaborators in person or message them through a personal phone, the fast-moving nature of financial markets limit the profit potential of such strategies.

Relocate a trader to their home office, however, and everything changes. Invisible to their colleagues for the vast majority of the day, they have a plethora of potentially unauthorised communication tools within easy reach and can effectively move off-grid within seconds of leaving the room. And while banks have been fast to authorise additional communication channels – most notably video-conferencing solutions like Zoom – in a bid to improve visibility and collaboration, data capture from these is so far patchy.

Consultancies have proposed various solutions, such as video-recording staff through the trading day and using facial-recognition software to trigger alerts when they leave their monitor for a certain period. But surveillance practitioners interviewed for this in-Focus Report voiced concerns about intrusion and consent, with one warning such actions could be interpreted as "productivity checking".

Remote working also creates additional conduct and information security risks that require new controls. For example, if the home is shared with other people, might they accidentally or intentionally access sensitive data related to the bank or its customers?

Model calibration

While surveillance teams' false positive problems have eased considerably since the first few weeks of lockdown, unusual working conditions make this an area that still requires immediate work, especially in the area of voice.

For example, banks need to calibrate their models to factor in new communication styles and talking points – which could be very different when risk takers are sitting in their family home compared with when surrounded by their peers on an informal trading floor. The

unprecedented nature of the pandemic and widespread homeworking (and therefore a lack of historical back tests) make this a challenging exercise.

AI and natural language processing could help and investment in these technologies is expected to rise as those banks that did not have access to smart filtering systems during the peak of lockdown panic seek to protect themselves from the fallout of any future market shocks and enjoy the cost benefits of outsourcing lower-priority alerts to lower-cost locations.

...if the home is shared with other people, might they accidentally or intentionally access sensitive data related to the bank or its customers?

Disparate data sources

The fluidity with which remote workers now move between an expanded pool of communication channels, sometimes within the same conversation, also creates fresh challenges for surveillance.

On top of global banks' long-standing headache of having to capture and analyse voice and e-comm data in a dizzying array of languages and colloquialisms, within a matter of months they have had to develop capacity and strategies for simultaneously doing this across multiple data sources.

"Surveillance teams now need to be able to monitor video-conference platforms, enterprise communication systems, collaboration tools and a host of other non-email, non-traditional chat platforms," notes Domash at Relativity.

"Behind every email address and username is a person sending a message. You need a system that can unify all these different data sources into a person communicating across channels. You need to be able to follow the flow of conversations as someone sends an email, then has a Slack conversation and follows up with a Zoom meeting. Being able to understand the context as the medium shifts from one platform is increasingly important."

Audit trails

Pre-COVID, a trend was already underway for surveillance teams to be located in geographically disparate clusters and to work at least some of the time from home. The transition to full-scale remote working has therefore been smoother than for traders and other risk owners with video-conferencing and regular team meetings helping support team cohesion, practitioners say.

It remains difficult, however, to replicate through scheduled calls the ad hoc collaboration and information sharing that physical proximity makes possible. While nearly 55% of attendees to a recent 1LoD Digital Debate agreed with the statement that Supervisors can be equally effective when their entire team is working from home, another 37% disagreed.

Practitioners interviewed for this in-Focus Report already use a variety of work-bench platforms, virtual whiteboards and case management systems to communicate with team members and manage alerts for various asset classes.

But the pandemic has created an increased need for more seamless, intuitive tools that allow for the sharing of context around cases as well as providing an audit trail into when and how team members review or escalate alerts, says Domash.

No free pass from regulators

From a regulatory perspective, banks have weathered the pandemic well, with compliance remaining robust across the sector as a whole.

Compliance practitioners say regulators in both the US and UK have been understanding about the challenges their functions face, and proactive in providing guidance, but that there has been no relaxation in terms of the standards they are expected to maintain.

Initial engagements with the UK's FCA, for example, were focused on how banks were coping with market volatility and the increased alert load, as well as their strategy for clearing them, whether that involved simple sampling or the application of AI filters. In its Market Watch 63 newsletter, released in May 2020, the regulator highlighted the importance of maintaining robust market surveillance and suspicious transaction and order reporting in a remote-working context to combat insider trading. It called on banks to review and update their risk assessments in response to coronavirus and to modify their surveillance systems where necessary to ensure they are properly calibrated to detect new or increased risks of market abuse.

And while regulators on both sides of the Atlantic have refused to offer banks a 'free pass,' practitioners say they have expressed a keenness to work with institutions to plug surveillance gaps and find innovative solutions for weak spots, as long as banks report them immediately.

> While nearly 55% of attendees to a recent 1LoD Digital Debate agreed with the statement that Supervisors can be equally effective when their entire team is working from home, another 37% disagreed.

Links to further reading

Relativity

[3 Ways to Adapt Your Surveillance Operations for a Remote Workforce]

[3 Steps to Building an AI Based Surveillance Strategy]

Making it permanent?

With most compliance practitioners predicting that remote working is here to stay, there is a strong argument for a wholesale review of surveillance controls and communication policies, and for today's makeshift workarounds to be replaced with long-term solutions and tech investments.

Having witnessed how smoothly many of their functions can be run remotely, banks are already questioning the logic of maintaining multi-storey offices in the world's most expensive cities, one practitioner noted. Surveillance teams are particularly well-suited to working from home most of the time, so are unlikely to return to the office at scale, most agreed. This makes a case for investment in smarter and more configurable collaboration tools.

For risk takers, the future is more uncertain. Even if solutions can be developed to plug gaps in the oversight of WFH traders and salespeople, the high-stakes nature of their function means banks will likely want them back in a controlled environment as quickly as possible, one practitioner argued. They may, however, be organised in smaller clusters, rather than in one centralised location, which will present fresh challenges for compliance.

And with health experts warning that the world could experience a series of localised waves of virus outbreak in the years to come, surveillance functions may have to build flexibility into their processes so they can seamlessly surveil traders as they move in and out of lockdown potentially several times. This also points to a risk that financial markets will experience a string of aftershocks, triggering further bouts of volatility that regulators will now expect surveillance teams to be prepared for.

Budget constraints vs investment

The chaos that COVID-19 has brought to financial markets and world economies has burned a hole in the balance sheets of many banks, making investment spend a hard sell to budget controllers. Surveillance practitioners warn that ambitious tech programmes already under way may be derailed by budget cuts. However, they say that they will continue to press for investments that create efficiency, for example by generating fewer false positives or communications to review, or that enable them to meet fresh challenges with the same or even reduced headcount.

Unusually, smaller banks, whose unsophisticated surveillance systems were least able to weather COVID-19's worst moments, may be more willing to invest in tech than their bigger peers in the months ahead, one practitioner believed.

Ultimately, this combination of pressures will force surveillance heads to be more strategic in their tech investments and to collaborate more closely with other functions such as IT, stressed one practitioner. For example, as new software or communication channels are introduced across banks, their impact on surveillance capabilities needs to be assessed from the outset, with solutions integrated before rollout rather than patched on later. Only then will surveillance teams be able to navigate fluid working practices and respond to future shocks at speed.