Video and Voice Surveillance Deep Dive:

HOW MUCH IS ENOUGH, AND HAVE BANKS GOT IT WRONG?

FORECAST 2023

smarsh® | 1LoD®

Key takeaways:

- Lack of regulatory prescription is an obstacle to investment in voice surveillance
- Banks consider the risks in voice channels to be lower than those in e-comms
- Only 9% of banks are very confident they're capturing all the audio they should
- Only 2% of banks consider video to be a significant repository of market abuse risk
- 17% of banks plan to prioritise investment in integrating voice and e-comms
- 16% of banks are capturing the video element of collaboration tools

Voice and video surveillance: How much is enough, and have banks got it wrong?

How do banks ensure that their voice and video surveillance processes achieve the right balance between risk mitigation, compliance, and cost, particularly given the paucity of regulatory guidance? And are they focusing too much on the issue of expense? At 1LoD's recent **Video & Voice Surveillance Deep Dive**, leaders from both the 1st and 2nd lines tackled those questions.

For regulators, the key issue in both e-comms and audio surveillance is whether the capture of information is complete. As one attendee put it, "We know that the regulator is extremely keen on this space at the moment from the point of view of data completeness. And I know it's something that our own internal audits focus on, whether it's for mobile providers capturing voice calls or turrets or whatever."

So, it is alarming that when asked about the extent to which banks are able to capture the necessary voice channels or data, only 9% of participants said they were very confident about their ability to capture what was required.

The surveillance minefield

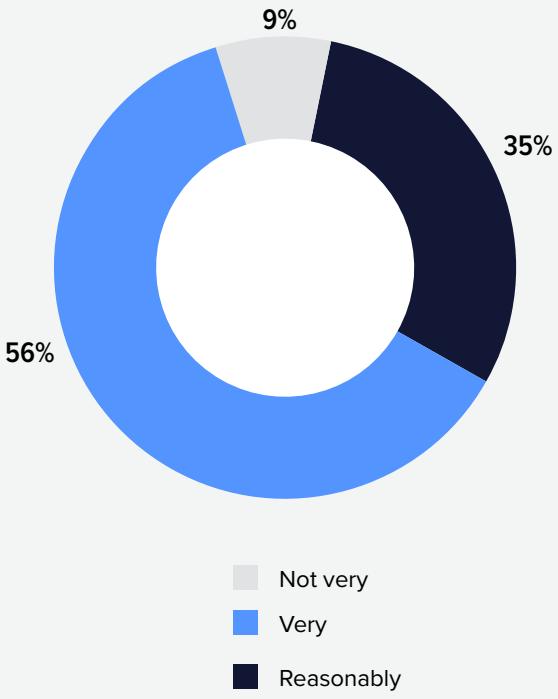
One problem with voice surveillance is that lack of prescription. As one attendee said, "There is no rule anywhere that says that comprehensive audio communications surveillance is a must. There are rules in certain jurisdictions that require you to record certain individuals. There are rules in the US that require a supervisory review, but that's generally a sample-based review. And about three times a year my auditors come and ask me to document the rules that specify in each jurisdiction that we have to do this; so, I then educate them on the fact that that regulation simply doesn't exist. Which I find a little odd given that we are all pretty clear that regulators expect us to monitor this stuff and banks are spending an awful lot of money on it."

This regulatory approach is a problem, and most surveillance heads want more prescription in this area. Not least, it would give them a stronger argument for resourcing. If they cannot point to specific regulatory requirements, teams tend to face push-back from the business and must come up with convincing reasons for additional spending. To do this, they must make the case that the risks justify the investment.

The case for voice

However, banks appear to be less concerned about the risk buried in audio. When asked which communication channels pose the greatest risk for market abuse, only 20% of attendees cited voice, whereas 73% identified instant messaging and other chat functions. Even taking into consideration the banks' (and regulators') natural tendency to fight yesterday's risks, this does not make it easy to pitch for more money.

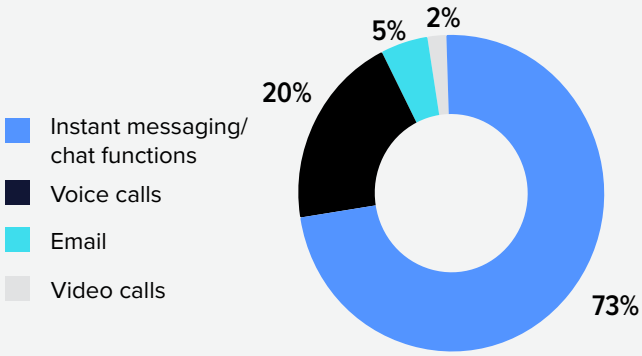
Are you confident that all voice channels/data that are required to be captured ARE being captured:



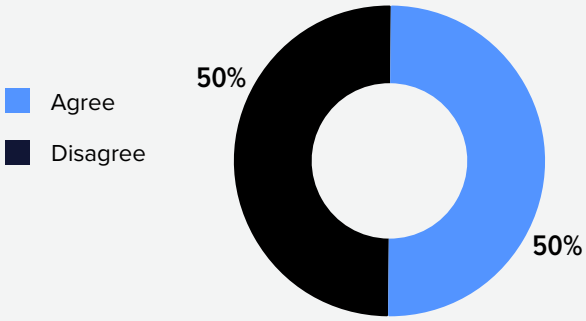
And debate participants agreed that in voice surveillance, the problem of false positives is often worse than in trade surveillance. “In voice it’s even worse because when you go away and listen to the recordings that have been flagged by a lower-level reviewer, most end up as being nothing. It’s very challenging when you spend a lot of money and then come up absolutely empty-handed at the end of it. You are better off making sure that you’ve got the pieces that are actually required under prescriptive regulation right, and that you’re not going to get fined for things you definitively should be doing,” said one participant.

This explains why only 50% of attendees said that they believe that the benefits justify the cost of investment in voice surveillance. It also explains why when asked, ‘Where is your organisation spending the majority of its new investment in surveillance in 2023’, only 9% cited voice, while e-comms and trade surveillance bag most of the budgets, and the integration of voice and e-comms account for 17%.

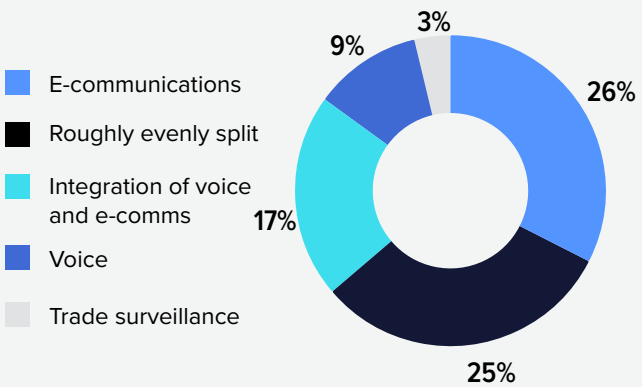
Which of the following communication channels do you believe pose the greatest risk for market abuse?



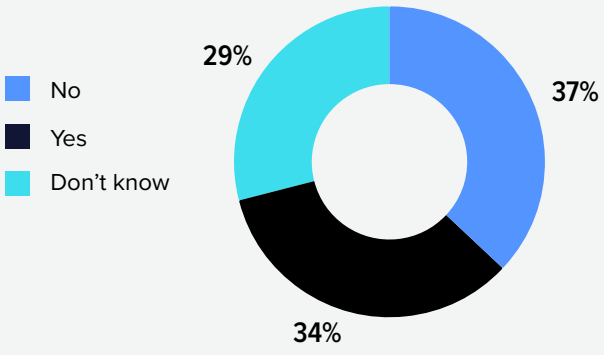
I believe that the benefits of voice surveillance I currently see today justify the cost of investment:



Where is your firm spending the majority of its new investment in surveillance in 2023?



My firm has replaced, or intends to replace, its legacy phone recording systems with an alternative solution in order to improve the data quality required by surveillance systems:



What about video?

Whether they justify it on the grounds of risk or cost, only 16% of attendees are capturing video, let alone conducting video surveillance. In fact, where banks have bought the technology to record everything from a Teams, Zoom or Webex meeting, the majority request that video capture is turned off and that only the audio (and sometimes the chat and other e-comms elements) are captured.

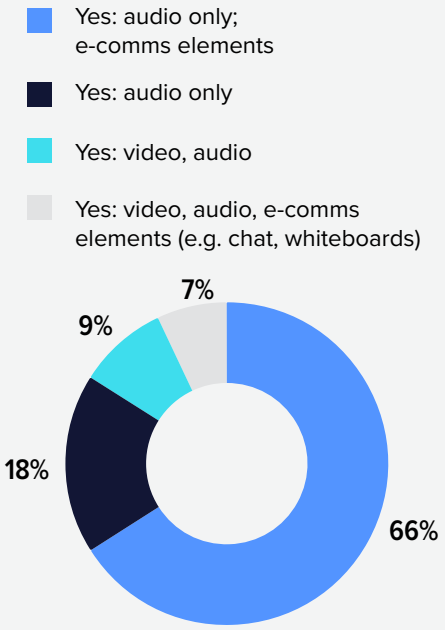
That is capture. What about the actual surveillance of video or its discrete elements? Asked whether their firms currently record and transcribe voice in video, only 17% said they are, while one third said they are developing the capability.

Why are banks turning off video capture, and why are many of them not even recording or conducting surveillance on the audio and e-comms elements? There are several reasons: regulators do not specify video capture; video storage is expensive; and banks may think that they can argue that the audio does not fall under existing audio capture regulation and that chat and whiteboards are not covered by existing e-comms regulations.

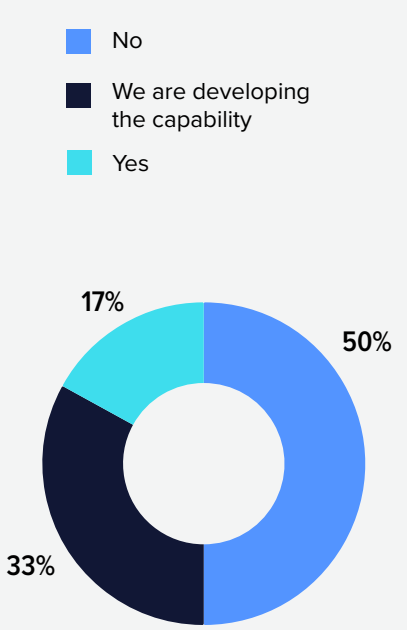
The lack of specific regulation leads to an approach that the banks describe as risk-based, but which sounds cost-based. Take the following comment on the subject of risk. “Now most front office client-facing and execution-based staff are in the office five days a week. So that risk of someone using the purely video aspect of a video call to communicate things that are not in the audio or chat, so hand gestures or waving documents, for example, is probably not as high risk as it might have been if they were working at home,” one participant said when justifying their decision to turn off video capture. “It’s a challenging environment for budget and we have many other things to consider when deploying technology.”

For the few who do actively carry out video surveillance, the most challenging aspect of preventing market abuse through video communications surveillance was ‘Identifying and analysing suspicious behaviours and patterns’, according to almost half of the attendees.

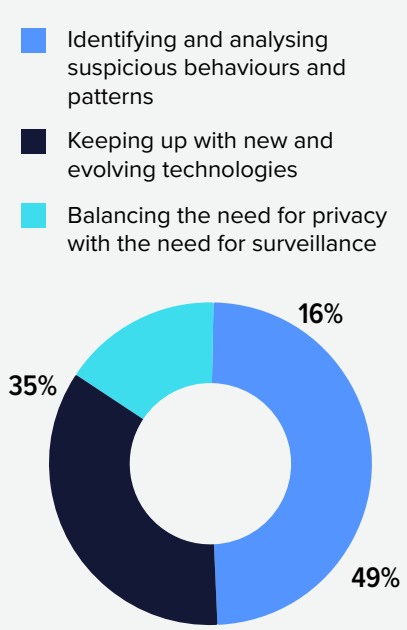
Do you capture any or all of the elements of video collaboration tools:



My firm is currently recording and transcribing voice in video communications:



In your opinion, which of the following is the most challenging aspect of preventing market abuse through video communications surveillance?



First, better language transcription and translation software. Banks know they are doing a partial job with multi-lingual surveillance and so, by definition, they are leaving risk on the table.

Covering the true risks: can tech help?

The worry is that both regulators and banks have got this wrong. The current approach focuses on solving the last crisis, not the next. It leaves an unknown level of risk undiscovered in the system. It ignores surveillance's potential for deterrence if rolled out to channels which are not covered. And it ignores the obvious point that bad actors will migrate to channels which are not monitored, and clients will move to those technologies which are easiest for doing business.

Banks recognise the issues. One participant explained, "We've done some analysis of regulatory actions over a nine- year period and found that 30% had an element of voice. That doesn't sound huge, but actually that was the largest channel – more than e-comms. So there clearly is risk in the voice channel. So, then the question is, can we mitigate that risk at an affordable price?"

Most attendees felt that two technologies were most likely to help. First, better language transcription and translation software. Banks know they are doing a partial job with multi- lingual surveillance and so, by definition, they are leaving risk on the table. Second, to get away from sampling and to improve detection rates in transcription generally, banks believe that improved natural language processing, or NLP, is the answer. "The ability to analyse natural language is radically changing and solutions are becoming much more accurate," said one attendee. "Obviously the cost-benefit is organisation-dependent, but these solutions look as though they will be able to deliver the ability to analyse all voice, not just samples, in a way that does not simply create yet more false positives."

This information was taken from the Video & Voice Surveillance Deep Dive on 28 & 29 March 2023.

smarsh®

1LoD®