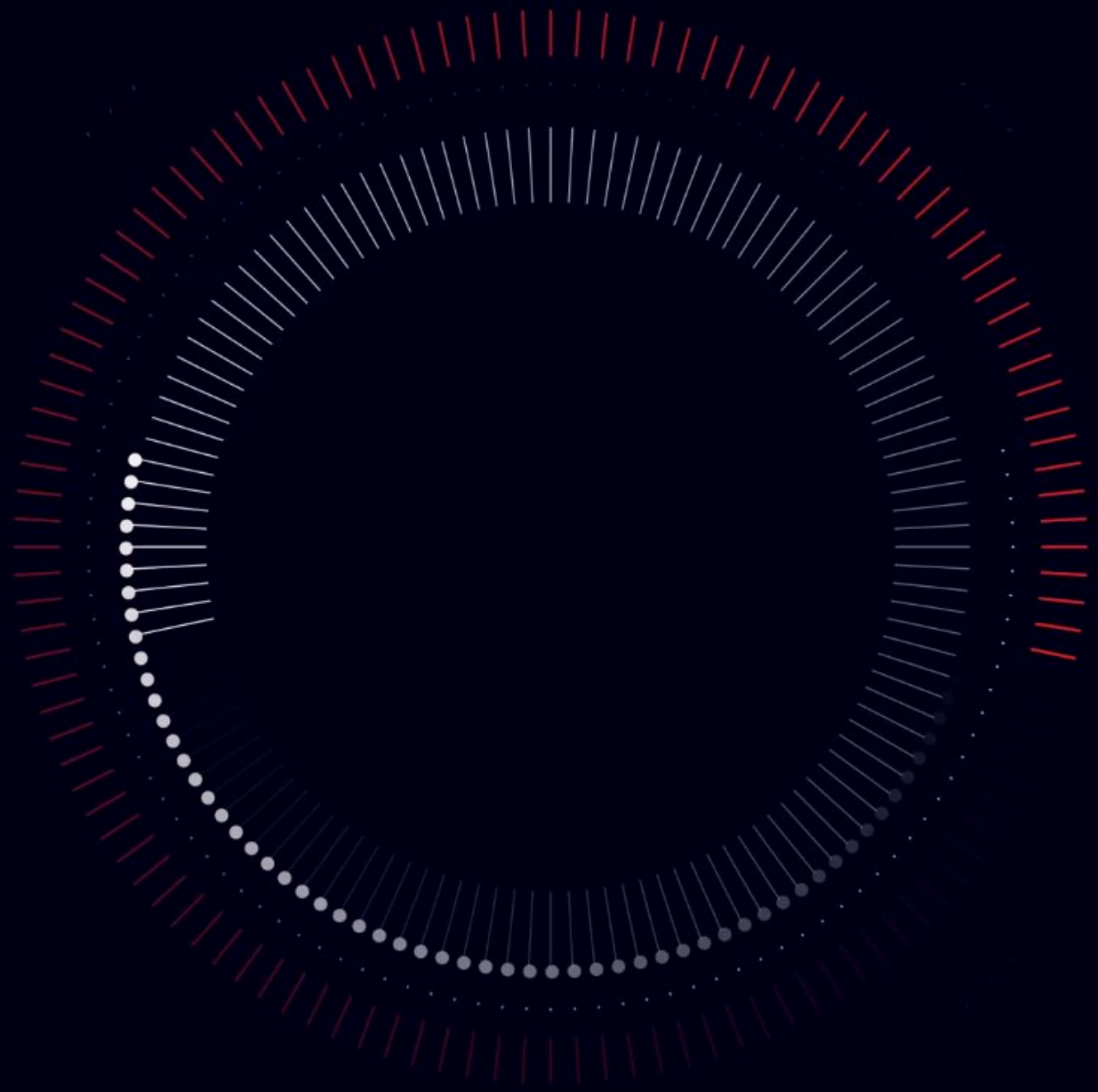
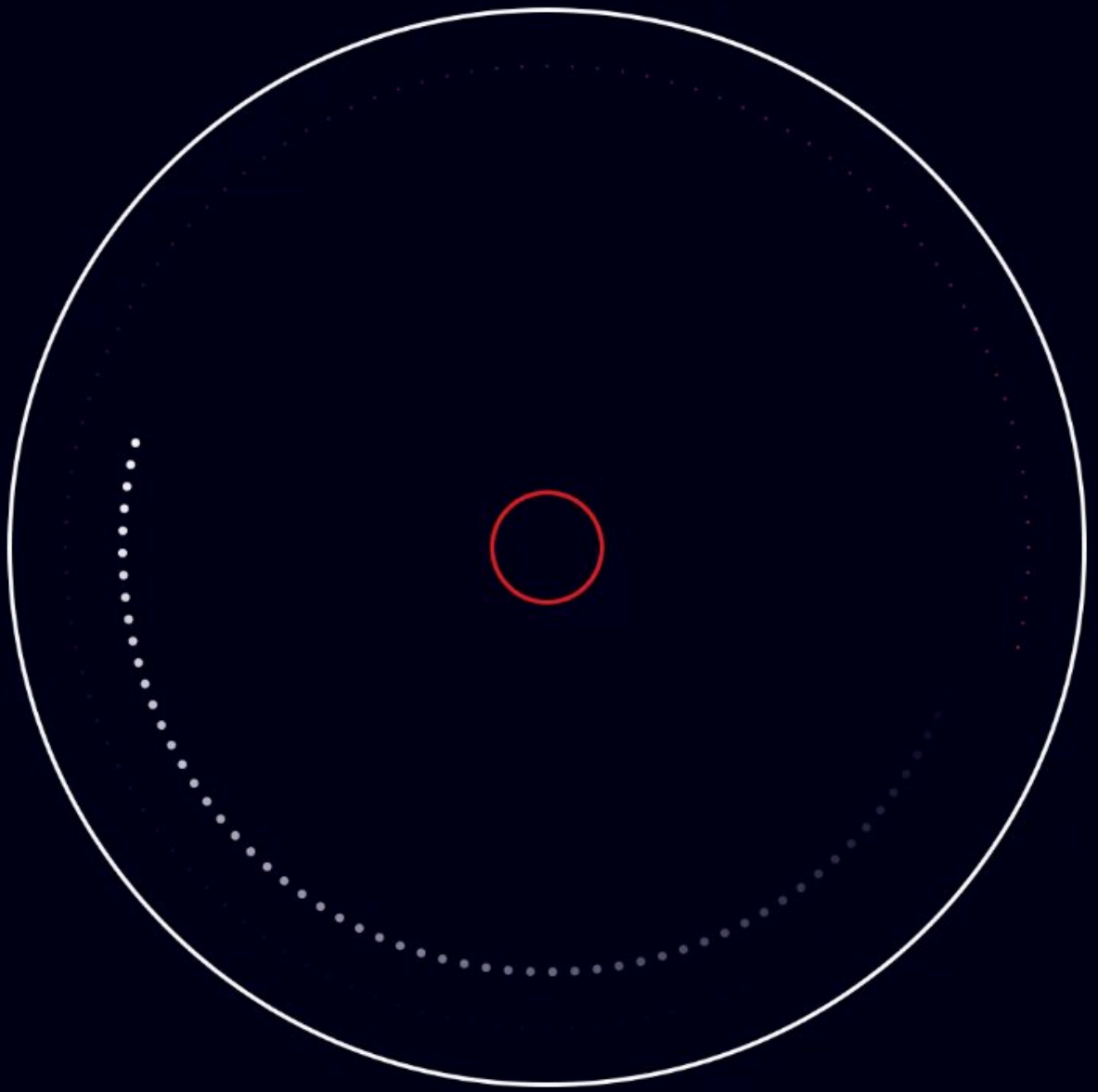
Global Relay Industry Insights

Compliant Communications Report 2024



About this report



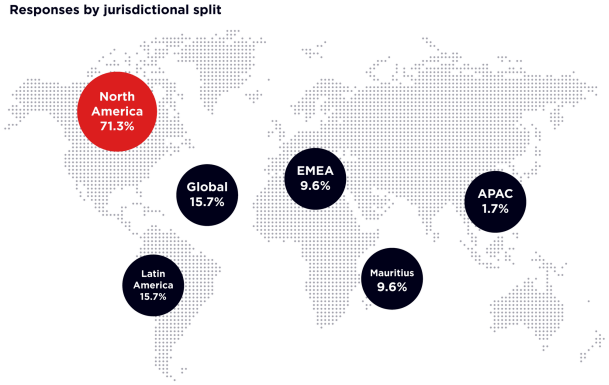
The Global Relay Industry Insights: Compliant Communications Report 2024 compiles and analyzes industry responses to regulatory action across recordkeeping, surveillance, and communication compliance.

Over two months in 2024, Global Relay issued an industry-wide survey with a view to find out how financial services firms are managing communication channels and emerging compliance trends. As well as exploring how firms are responding to continued regulatory enforcement action for off-channel communication, we wanted to understand how organizations are incorporating solutions such as AI and communications surveillance into their existing compliance workflows.

The survey generated responses from critical roles, from Chief Compliance Officers and Chief Data Officers, through to Head of Risk and Supervision, Heads of Surveillance, and Compliance Officers.

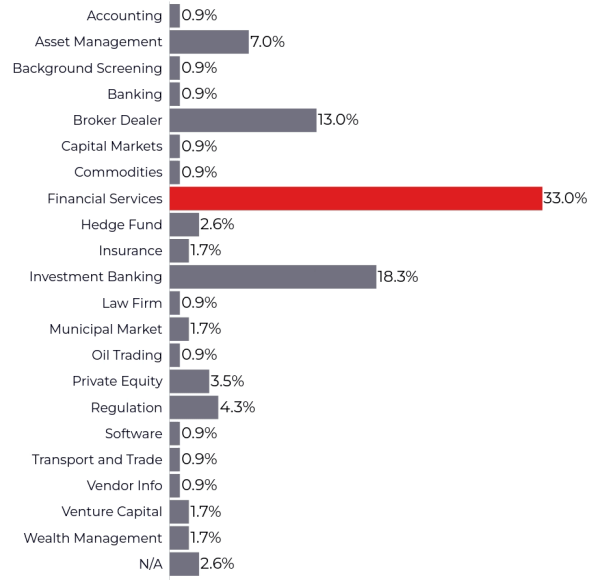
We received responses from professionals working around the globe, with the majority working within North American or global financial organizations.

Responses by jurisdictional split



The survey was aimed at financial services generally, but gleaned multiple responses from industry subsets including Asset Managers, Broker Dealers, and Investment Banks.

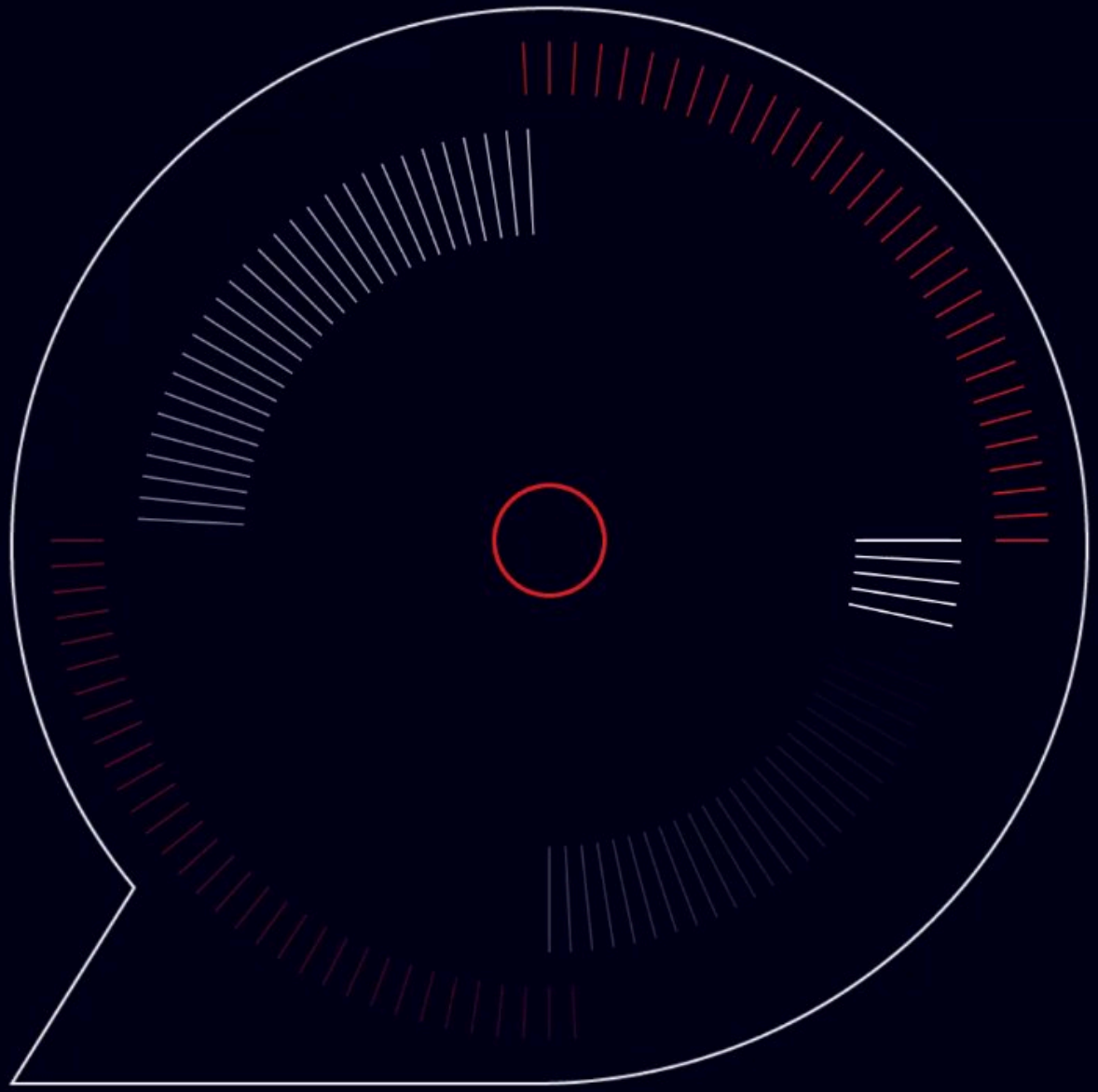
Responses by industry split



This report explores the current landscape for compliance to lift the lid on the challenges that financial institutions are facing, and the steps they need to take to remain compliant in the future.

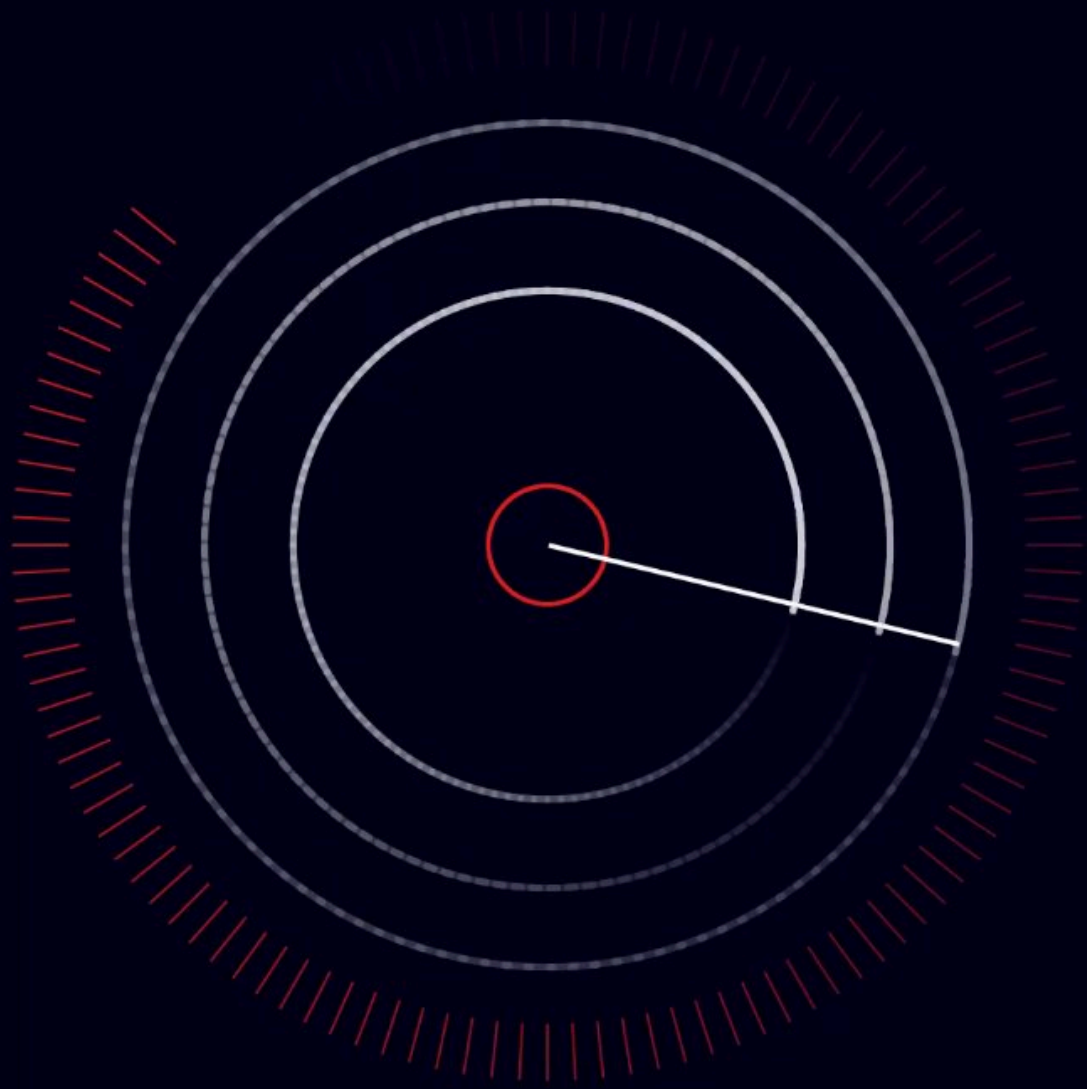
Foreword

A message on compliant communications from Alex Viall, Chief Strategy Officer, Global Relay




Welcome to our
Industry Insights report for 2024.

Key findings



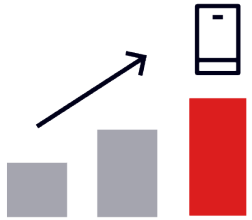
43.5%

of compliance teams continue to ban WhatsApp and WeChat, despite further regulatory enforcement action (and they're still not confident it's effective)

65.2%

of respondents said that getting employees to comply with rules for electronic communication is their biggest challenge. This has increased from **61.5%** in 2023

BYOD policies are more common than ever, increasing from **51.3% to 66.8%** in a year



55%

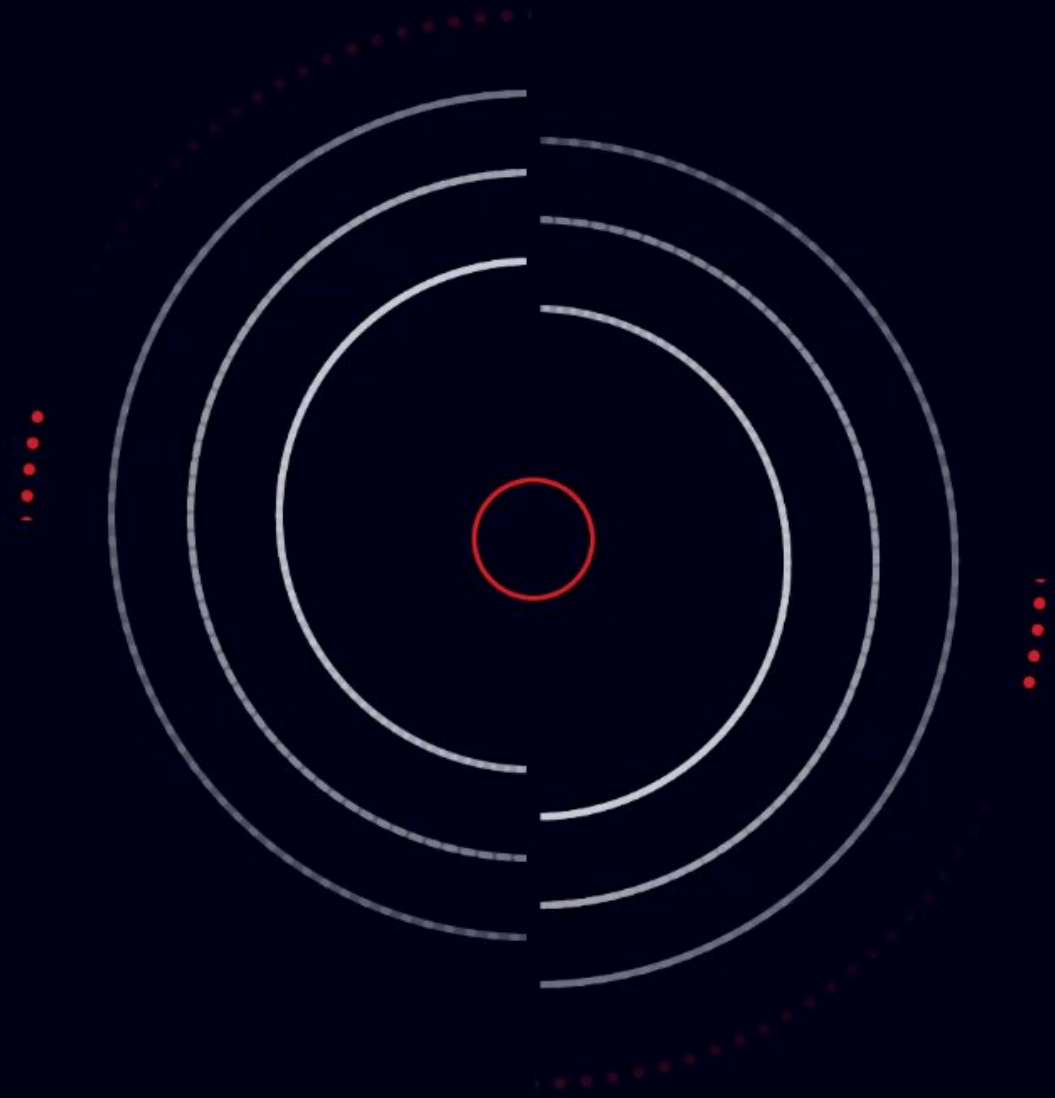
of financial institutions consider social media to be an emerging compliance risk

42%

of respondents plan to introduce AI into compliance workflows in the next year. But **65%** of North American firms don't plan to use it

Channel bans and unclear plans

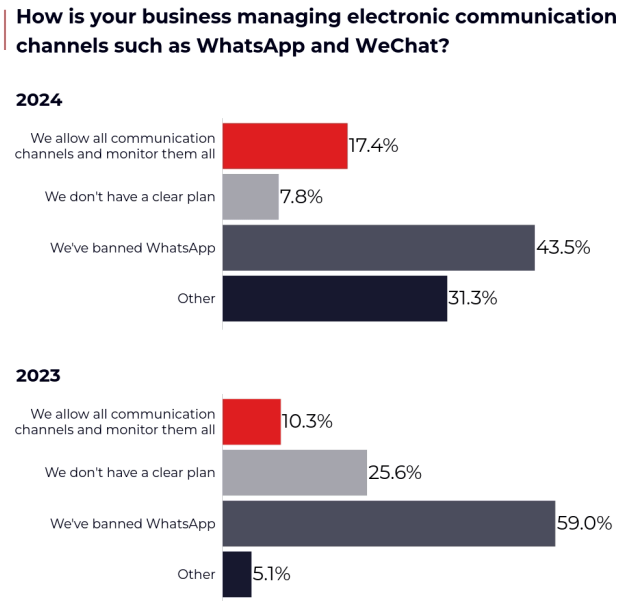
How are businesses managing electronic communication channels including WhatsApp and WeChat?



Channel bans still prevail

Global Relay Industry Insights Report: Compliant Communications 2023 found that, in response to enforcement action from U.S. regulators, 59% of respondents had opted to ban WhatsApp and WeChat. Despite the majority opting for channel bans, 56% said that they did not believe channel bans to be an effective solution.

At the time, only 14 months after the U.S. Securities and Exchange Commission's (SEC) landmark fine issued to J.P. Morgan Securities LLC, there was an assumption that channel bans were being used as a stop-gap while firms sought to implement tools and systems that would withstand regulatory scrutiny.



In 2024, channel bans continue to prevail as the most common solution for WhatsApp, with 43.5% of respondents continuing to ban WhatsApp for business purposes. Consistent with results in 2023, those who have implemented such bans are uncertain as to whether they are effective.

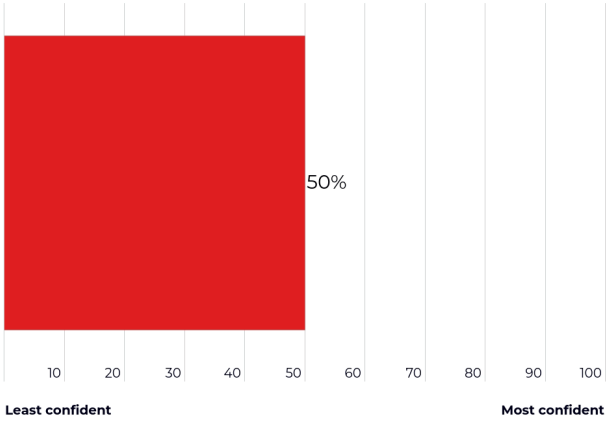
Alex Viall,
Chief Strategy Officer,
Global Relay

I am not that surprised that the WhatsApp total ban policy prevails, but think it is interesting that it's decreasing, which shows there are more technology solutions available after the initial panic as the SEC and CFTC started their rolling enforcement.

My interactions with the market suggest that compliance people know that a ban does not mean the monitored population won't use unapproved channels. I think many know they ultimately have to enable this type of communication, in a compliant way, as it is a business advantage.

I do think, however, that awareness around the risks and expense of non-compliance, both at a personal but also corporate level, has increased radically since last year. This messaging and policy is coming right from the top – the enforcement actions are having a significant deterrent effect and the attitude that a regulatory fine is just a cost of business is changing. The fact that we're seeing bonuses reduced where fines are levied on firms, implicitly passing cost onto non-compliant employees, goes to prove this. Bigger fines do focus the mind.

How confident are you that banning communication channels is an effective solution?



More than two years since the SEC's first enforcement action in this area, it is unlikely that organizations are continuing to ban WhatsApp as a "quick fix." Instead, channel bans appear to be in place as a long-term solution, despite questions around their compliance credentials.

Since the publication of last year's Industry Insights Report, U.S. regulators have continued to issue considerable fines to firms that "did not maintain or preserve the substantial majority of these off-channel communications." This includes a combined penalty of $289 million to 11 firms in August 2023, where "employees often communicated through various messaging platforms on their personal devices, including iMessage, WhatsApp, and Signal, about the business of their employers."

It also includes a combined penalty of $79 million issued to 10 firms that failed to capture business messages sent from personal devices in September 2023, and a combined $81 million penalty issued to 16 firms in February 2024.

Despite this continued action, we see firms enacting solutions that they do not believe to be watertight, exposing themselves to vulnerabilities and regulatory scrutiny.

Trending towards compliant solutions

While 43.5% of respondents said that they have banned WhatsApp, 2024's survey results show a gradual shift towards the compliant implementation of solutions.

In 2024, only 7.8% of firms say that they do not have a clear plan in place to tackle off-channel communication channels, such as WhatsApp. This has fallen since 2023's report, in which far more compliance teams said that they did not have a plan (25.6%). This shows that, though compliance solutions may not yet have been implemented, plans have been formulated, and fewer organizations are uncertain as to how to manage off-channel communications.

Moreover, 10.3% of 2023's survey respondents said that they allow all communication channels, and monitor them all. This has increased to 17.4% in 2024.

While only a move of around seven percentage points, this again points to a shift in approach whereby organizations are implementing compliant solutions that allow for the capture, storage, and monitoring of all relevant business communication channels.

This broadly aligns with the findings of Global Relay's Data Insights Report in 2023 which analyzed the data of 10,000 financial services firms to understand the communication channels they were capturing.

This report found that, over the course of five years, purchasing decisions for compliance technology had increased significantly. In particular, firms have made significant investments in the capture of communications data across fast-emerging communication channels, including WhatsApp, SMS, and LinkedIn.

Industry insights

"We allow WhatsApp if the employee consents to archiving. Unarchived platforms may only be used for logistical communications."

Private Equity,
North America

"We're using Global Relay's Messaging App which allows sending WhatsApp messages from a business phone number that is monitored."

Director of Compliance,
Financial Services, North America

"We allow WhatsApp using a wrapper solution so communications are archived."

Chief Compliance Officer,
Asset Manager, North America

"I oversee the rigid implementation of a specific internal company communications policy which outlines the approved platforms."

Chief Compliance Officer,
Asset Manager, Global

"We require WhatsApp communications to be captured and saved by employees."

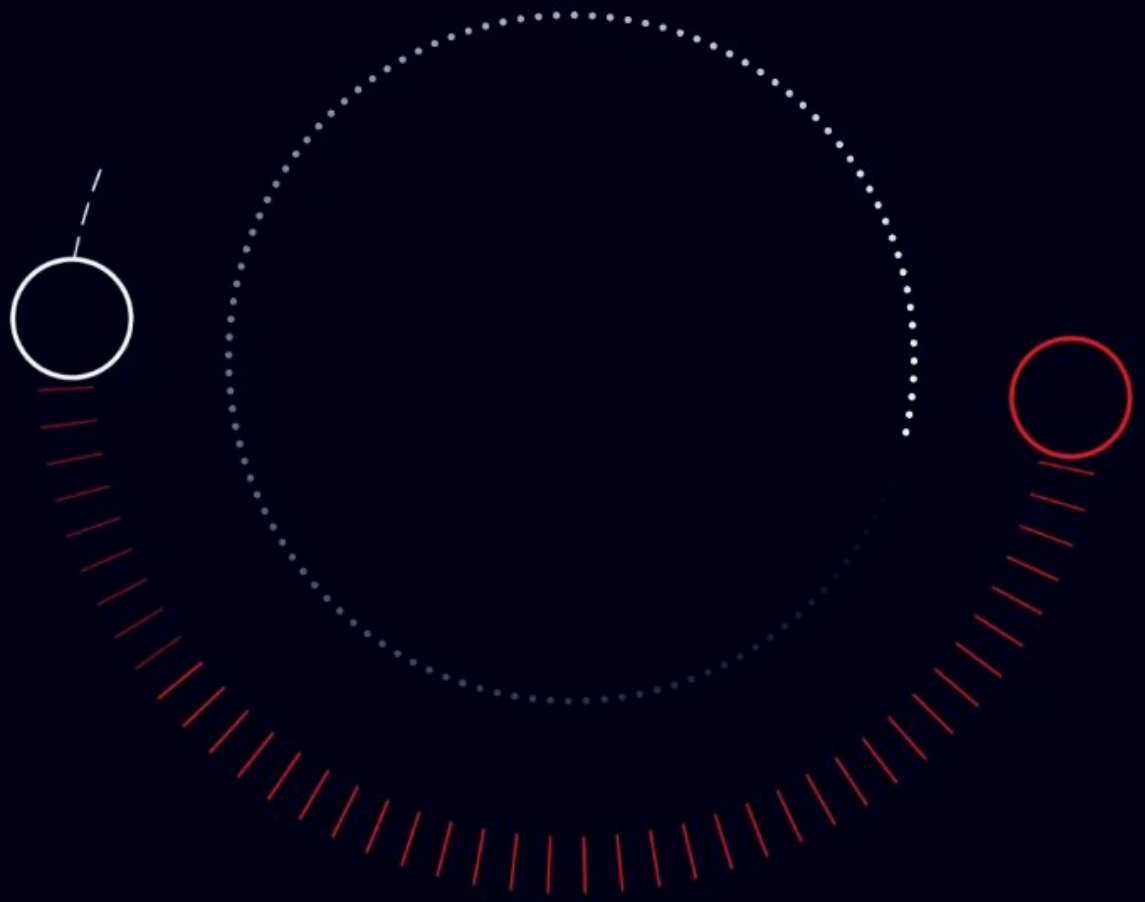
Chief Compliance Officer,
Venture Capital, Global

"Policy directs what comms are permitted and clearly indicates any new tools must be approved by Compliance."

Director of Compliance,
Insurance, North America

Concerns around communicating compliantly

What is the highest priority when ensuring compliance with electronic communication channels for business activity?



Behavioral issues

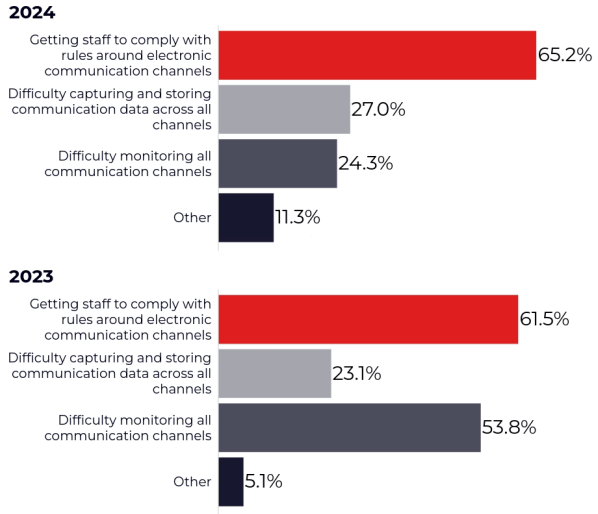
The most prevalent non-compliance issue within regulatory enforcement action for off-channel communications is a behavioral one. It is seldom a lack of rules or policies that causes non-compliance, but an individual's unwillingness to follow them.

> **The hardest task is persuading people to change their behavior. They don't break the rules because they don't know or understand them.**
>
> **Carroll Barry-Walsh, Lawyer, Speaker, and Founder at Barry-Walsh Associates**

In 2024, 65.2% of respondents have said their biggest concern when ensuring compliance with communication channels is "getting staff to comply."

This figure has increased by 3.7 percentage points, up from 61.5% in 2023. One year on, the issue of instilling a culture of more compliant behavior not only persists, but is apparently more challenging.

What is your highest priority when ensuring compliance with electronic communication channels for business activity?*



*This was a multiple choice question, so the numbers won't add up to 100%

As regulatory scrutiny increases alongside stricter policies within firms, it is interesting to note that human behavior is becoming more of a concern than it was in the year prior. This is especially true given that regulators are at pains not only to take enforcement action against financial organizations, but against the non-compliant individuals within those organizations.

> Individuals are increasingly being held to account for their non-compliant actions, yet compliance teams still struggle to get “employee buy-in” with policies and procedures.

Rob Mason, Director of Regulatory Intelligence, Global Relay

“This may be because we are understanding employee behavior more, and have more awareness generally because of the ongoing ‘compliant comms’ issue.

This is also a testament to the fact that we all spend huge amounts of time on mobile phones every day.

As the lines between personal and business communication can easily blur, instilling discipline on the basis that compliance may not know if I use my personal mobile to influence business in some way means it is challenging to maintain a complete data set.

Carroll Barry-Walsh, Lawyer, Speaker, and Founder at Barry-Walsh Associates

Why is it so hard to get staff to comply?

Bluntly: Mixed messages. Companies are asking staff to use a variety of communications channels to respond promptly. Make something easy and quick to use and staff will use it. At the same time, they don't want staff to say dumb things.

How to square this circle? The key message which needs drumming in over and over is that these are work channels for work purposes and that staff must behave professionally. Professionalism is the key – rather than simply compliance with rules.

Act professionally. Speak professionally.
Write professionally.

That is what staff need to hear from bosses and need to understand and internalize for themselves.

What does this mean in practice?

Three golden rules:

1. Do you really need to write this down? And in this way? THINK before pressing 'send.'

2. If your communications are being read, it's because something has gone wrong. So don't write stuff down you're not prepared to defend years later.

3. Non-work comments: if you wouldn't like your mother reading it, don't write or send it.

When employers talk about bringing your 'whole self' to work they do not mean your sex life, private fantasies, or personal thoughts about others, no matter how witty or amusing you think you're being. 99% of what is in your head is not worth making public in a professional environment – and probably not anywhere else either.

Bad examples are worth sharing with staff to show them what is on the wrong side of the line.

Technical difficulties

Away from issues of human factors in non-compliance, multiple respondents highlighted technological challenges as their current priority.

Regulators, especially those in the U.S., have made clear their zero-tolerance approach to firms that fail to preserve business communications. However, while regulatory expectations are clear, technological solutions still appear to cause a degree of uncertainty.

In 2024, the number of respondents that said they have difficulty capturing and storing communication data across all channels has risen by 3.9% to 27%, up from 23.1% in 2023.

Conversely, 23.4% of respondents said that they had difficulty monitoring all communication channels in 2024, which has decreased significantly from 53.8% in 2023.

Rob Mason, Director of Regulatory Intelligence, Global Relay

Communication channels continue to spring up. Front office colleagues like to be able to accommodate their clients and so are keen to chat to them on the channel of communication of the client's choosing.

The number of these used to be fairly limited, but now this could include a whole deluge of channels, for example, Bloomberg, Refinitiv, Symphony, ICE chat, Teams, Zoom, Slack, CME, Cisco, Skype, and that's clearly not a full list...

Firms are also thinking about other channels such as social media, for example, LinkedIn, Facebook, Instagram, X (formerly Twitter), YouTube, TikTok, etc.

So immediately you can see there's a challenge to getting that data into relevant systems so it can be monitored as well as the recordkeeping aspects of all business activities... there seem to be new comms channels popping up all the time!

Technology does provide this capability, but the data Connectors which are the clever pieces of kit that can accommodate all the different channels and data anomalies within those channels and uniformly format and index data and make sense of it safely and securely, is a very specialized discipline.

Strong technology solutions and the flexibility of those solutions are critical to accommodate these and new channels as they inevitably arrive. Testing these too – routine testing or MI to assure completeness to the client.

> **This all comes down to technology. Technology has improved to make it simpler to monitor or supervise communication. But it is also technological innovation that means there is always a new compliance tool to capture, making that harder simultaneously. Technology is to blame – for both the good and the bad.**
>
> **Pankaj Anand, Head of Governance Technology Solutions, StoneX**

With a constantly changing communication ecosystem, firms are consistently tasked with finding solutions to capture new – or previously unused – communication channels.

As an example, in 2023 an individual was charged with insider trading after sharing inside information on Xbox 360 voice chat. As employees take up new means of communicating, firms will naturally be on the back foot with solutions.

Industry insights

What's your biggest compliance challenge?

"Sifting through the vast amount of 'noise' and false positives captured by e-surveillance tools. I would be interested to see how AI can (or has already) play a role in this space."

Chief Compliance Officer,
Hedge Fund, APAC

"Any policy only works when people comply – our staff is great about this – all electronic comms are copied into email (and replied to from there) and captured with Global Relay."

Director of Compliance,
Financial Services, North America

"Making the institution understand the real risk involved and addressing the matter properly."

Senior Monitoring and
Surveillance Analyst,
Broker Dealer, North America

"Ensuring staff knowledge of the policies and consistency in application across the business. Do what we say we are doing?"

Vice President of Compliance,
Asset Manager, Global

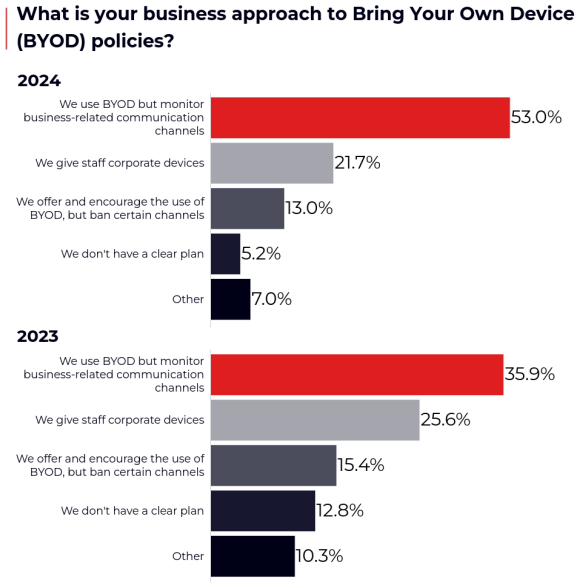
The rise and fall of Bring Your Own Device

Have Bring Your Own Device (BYOD) approaches changed in light of regulatory fines?

BYOD is more common now than ever

The operational benefits of Bring Your Own Device (BYOD) policies are well documented. From financial benefits, to ease of use, in a world that has seen considerable shifts towards more hybrid ways of working, BYOD prevails.

In response to regulatory enforcement action for firms who failed to preserve business communications made on employees' personal devices, industry speculation suggested there would be a sharp shift away from BYOD to corporate-issued devices. According to survey responses, however, this perception is incorrect.

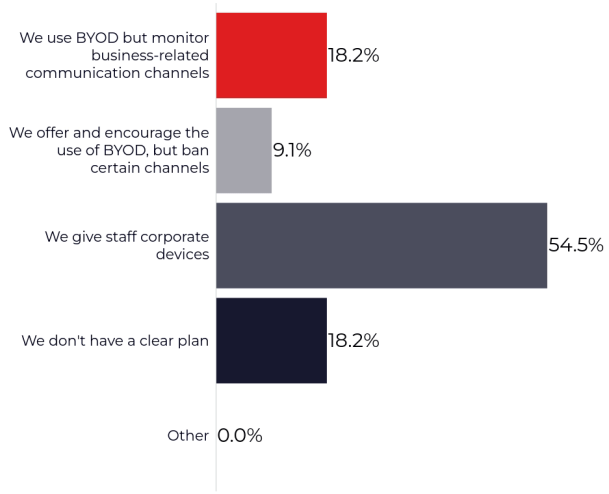


Since our 2023 Industry Insights Survey, the number of organizations that offer a BYOD model for business communications has risen by 17.1 percentage points, from 35.9% to 53%. Similarly, the number of firms issuing staff with corporate devices has decreased, from 25.6% in 2023, to 21.7% in 2024.

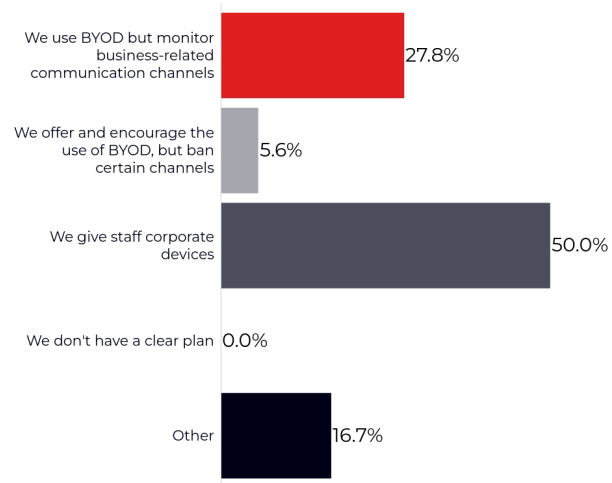
> **I am a little surprised that BYOD usage is still topping a shift to corporate device policy. What I have noted in many of my roundtables is that many firms are separating their corporate populations into high-risk and not so high – it is the high-risk monitored population that are all being moved to corporate devices and BYOD is good enough for the rest.**
>
> **Alex Viall, Chief Strategy Officer, Global Relay**

When broken down by jurisdiction, there is a clear divide in how financial organizations approach BYOD vs. corporate-issued phones. Notably, 54.5% of firms based in EMEA favor corporate devices. This is also true of 50% of global firms. Firms based in North America have a clear proclivity towards BYOD policies, with 63.4% noting that they use a BYOD model and monitor business-related communication channels. Only 11% of North American firms said that they give staff corporate devices.

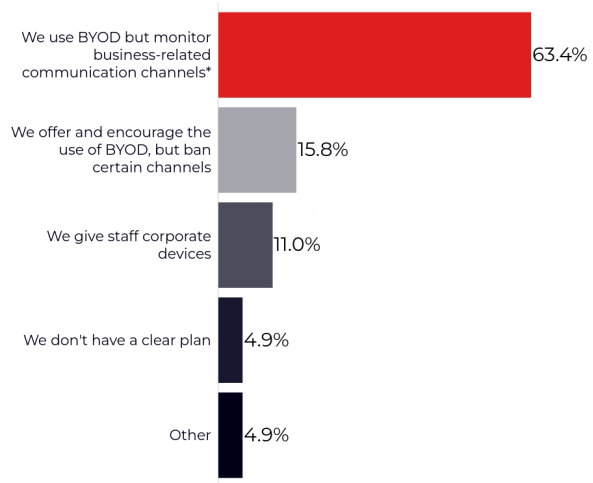
EMEA: What is your business approach to Bring Your Own Device (BYOD) policies?



Global: What is your business approach to Bring Your Own Device (BYOD) policies?



North America: What is your business approach to Bring Your Own Device (BYOD) policies?



*BYOD most prevalent in the US

Martin Gaterell, Associate Director: Private Side Advisory with Monitoring & Surveillance, Unicredit GmbH

We have always operated on corporate devices only for those in scope and risk relevant. The reason this is our preferred option is I expect the same reason people are either moving away or refreshing, which I expect is a synonym for 'tightening' up the rules, it is plainly about control.

Our corporate devices give us control on the channels in use and what they are used for. There is a big decision to be made by the industry regarding the surveillance of personal mobile devices. Especially as we have seen the U.S. regulators subpoena personal devices in recent times. Also, there are DPO issues to be considered in this context which acknowledge the different country requirements.

Chip Jones, Executive Vice President, Compliance, Global Relay

I guess I'm not surprised that BYOD is more popular with financial services firms in the U.S. Corporate devices versus BYOD really boils down to Three C's – Cost, Compliance, and Convenience.

Regarding 'Cost' – corporate devices are much more expensive than BYOD. With respect to U.S. broker-dealers, the choice can usually be segregated easily by business model. Your large employee-based firms have distributed corporate devices. Whereas your independent contractors have adopted BYOD policies. Given that there is no empirical evidence that corporate devices are more compliant than BYOD, firms will choose the device that works best for their business model.

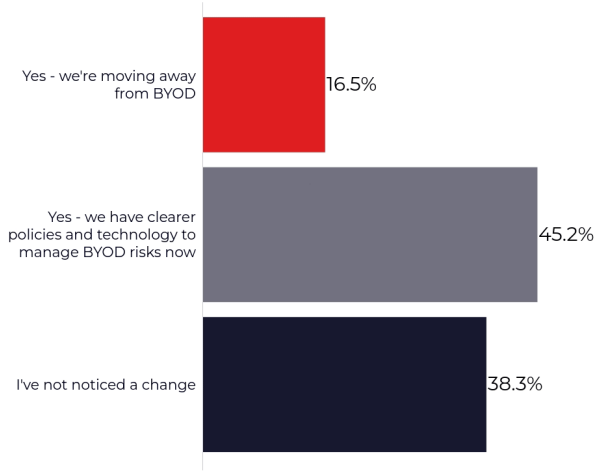
Regarding 'Compliance' – I think there used to be a perception that corporate devices were more compliant than BYOD. This is simply just not the case and firms now realize that both corporate and BYOD devices can be equally compliant. With a corporate device, investment professionals can distinguish easily between their work phone and personal phone. Due to technological developments and compliant communication apps, the same can now be said for BYOD.

Regarding 'Convenience' – The financial professional wants to do whatever makes it easier for them to communicate with their clients. Now that the SEC has focused the spotlight on these communications, financial services firms have driven the point home with their representatives that compliance in this space is extremely serious. Now the representatives understand the seriousness but are saying – "make it easy for me." Well, it is much easier now. With the products and tools that have been developed by vendors such as Global Relay, it simply boils down to the fact that employees must be trained to use the correct phone number associated with the compliant business communications – whether that be a corporate or BYOD device.

All change, or no change for BYOD?

Given the strength of speculation around a potential shift away from BYOD, we asked firms whether they had seen the use of such policies change in light of regulatory enforcement surrounding personal devices. Fewer than expected said that they were moving away from BYOD by reason of regulatory action, at only 16.5%.

Have you seen the use of BYOD policies change in light of regulatory enforcement actions concerning personal devices?



Instead, it appears that organizations are revisiting their existing BYOD policies to make them clearer, and stringent enough to meet shifting compliance expectations. 45.2% said that they were looking again at existing policies, while 38.3% had not noticed any change. This would suggest that, instead of ripping up the rulebook and investing in corporate devices – at huge cost to the organization – firms are taking the time to rewrite the rulebook and ensure it is clear and understood by staff.

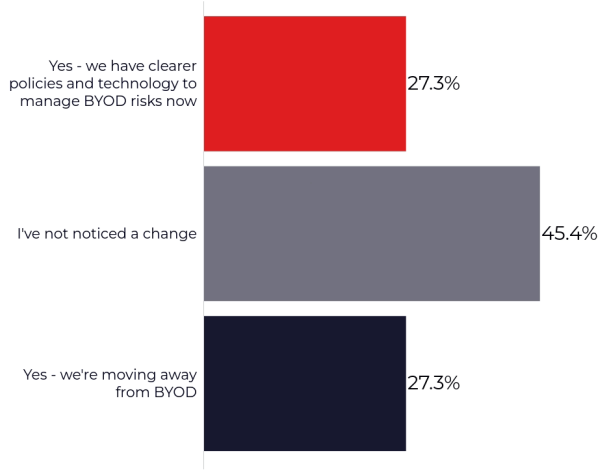
Pankaj Anand, Head of Governance Technology Solutions, StoneX

From what I've seen, companies have been reassessing their BYOD and corporate phone policies over the past few years, most probably driven by COVID to some degree.

This shifted behaviors, and the challenge has been in resetting those behaviors again. For instance, when issuing corporate devices to client-facing teams, they don't necessarily like it because they now have to have two phones, which is a pain. But it's training that behavior of 'work phone for professional life, personal phone for home life.' And we've just had to adopt a very strong position with it.

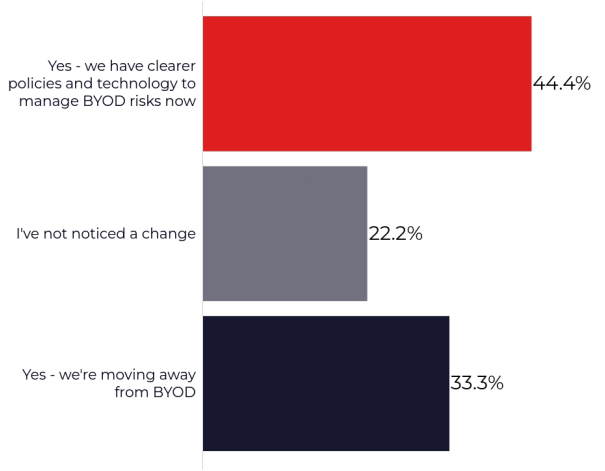
Since the big fines in the U.S., I've definitely seen a shift towards even tighter policies, but also towards new investment in corporate devices – often at considerable expense. It makes a clear demarcation between personal and professional channels. People are definitely starting to get the message about the importance of comms governance since the fines.

EMEA: Have you seen the use of BYOD policies change in light of regulatory enforcement actions concerning personal devices?



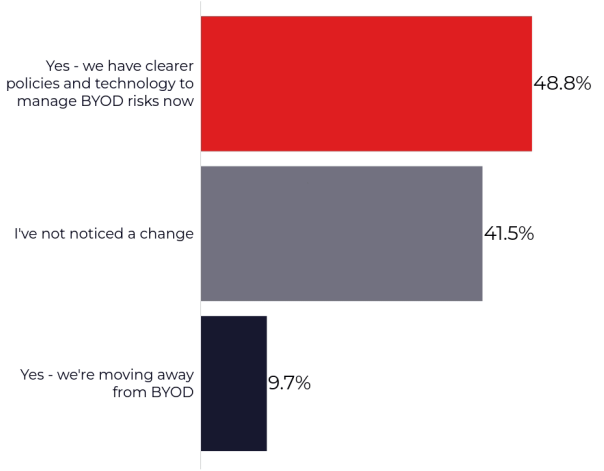
Once again, changes – or apparent changes – to BYOD policies in response to regulatory scrutiny vary by jurisdiction. 45.4% of EMEA-based respondents, and 41.5% of North America-based respondents said that they had not noticed any change regarding BYOD.

Global: Have you seen the use of BYOD policies change in light of regulatory enforcement actions concerning personal devices?



Conversely, 22.2% of global respondents agreed. This is of particular interest given that North America has seen the most intense regulatory scrutiny around off-channel communications.

North America: Have you seen the use of BYOD policies change in light of regulatory enforcement actions concerning personal devices?



Again, only 9.7% of North American firms said they are moving away from BYOD, though 48.8% are revisiting their policies. EMEA, on the other hand, sees 27.3% of respondents moving away from BYOD policies, despite seeing the least regulatory messaging on this topic.

Industry insights

What's your approach to BYOD?

"We apply the same security metrics to BYOD as we do to corporate-issued devices."

Chief Financial Officer,
Investment Bank, North America

"We use BYOD, but corporate 'apps' are ringfenced from the rest of their device and centrally monitored (i.e. MS Outlook, Teams)."

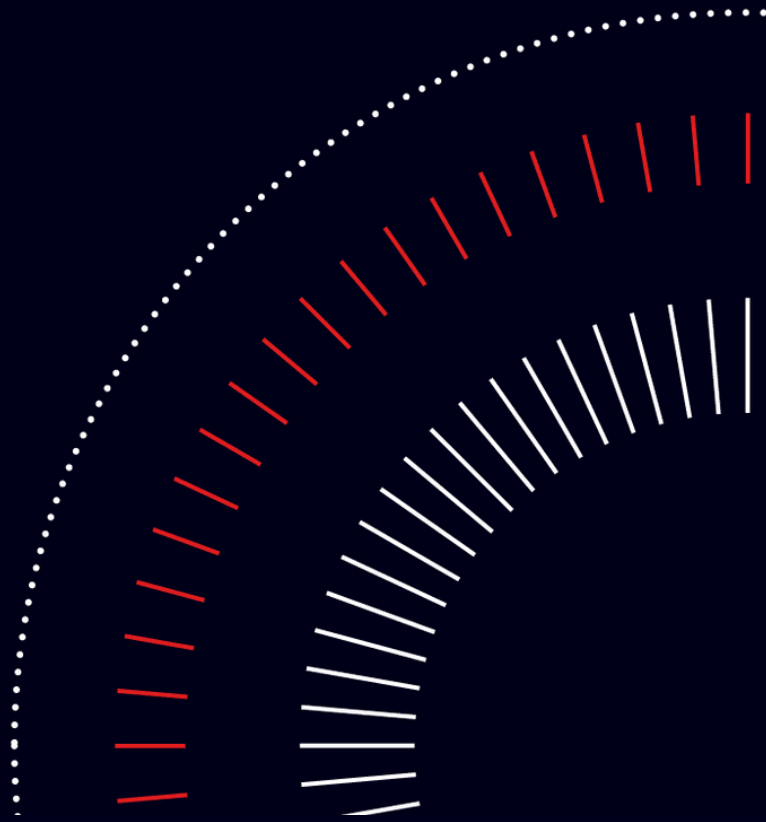
Chief Compliance Officer,
Hedge Fund, APAC

"We require preapproval for BYOD to ensure we can monitor."

Compliance Officer,
Hedge Fund, North America

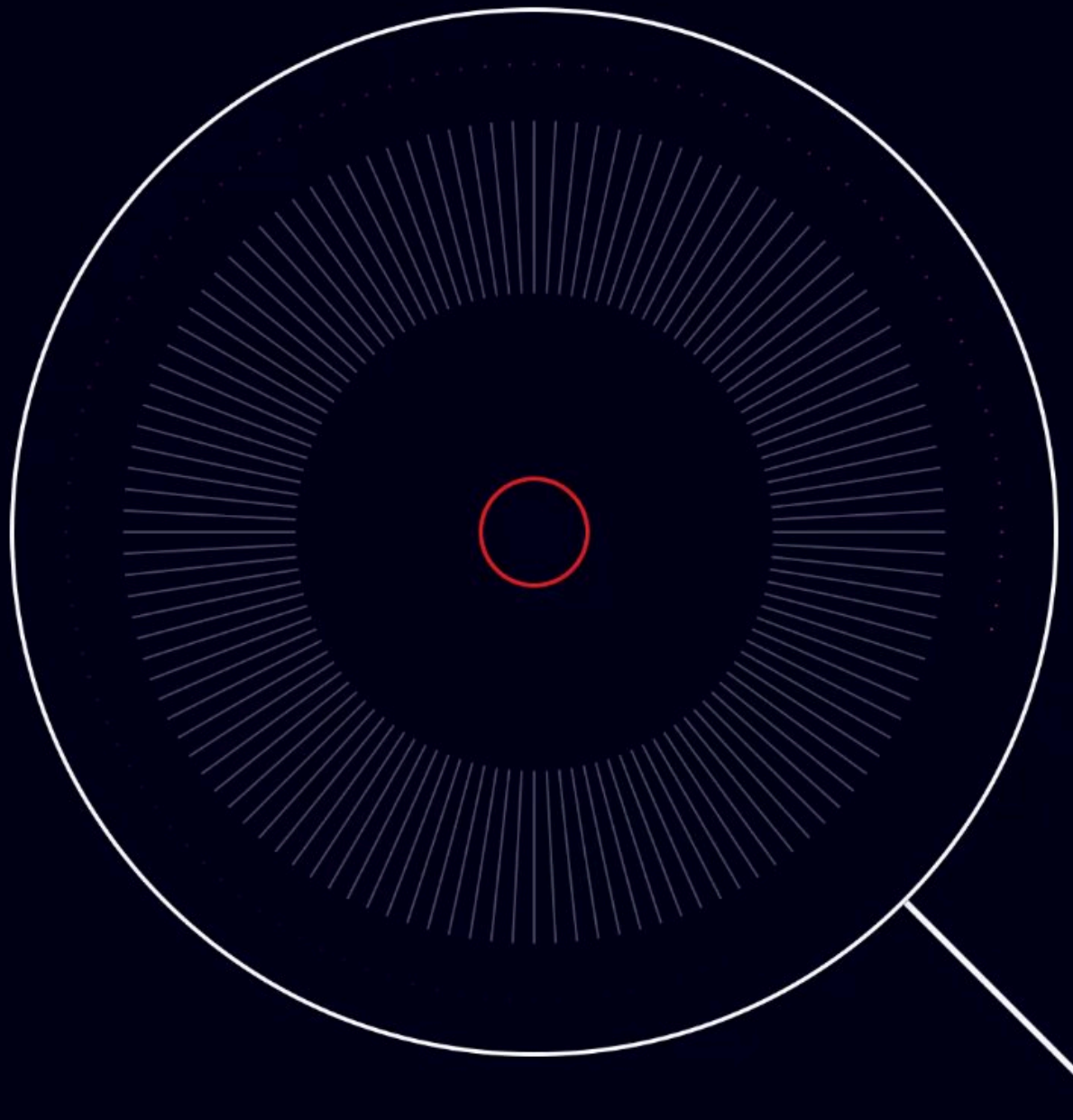
"If anyone contacts me personally on any social media site or on my personal cell phone, I explain we need to communicate on business platforms."

President,
Insurance, Global



U.K. regulators and compliant communications

Are businesses worried about increased action from U.K. regulators?



A recap of the FCA's stance on recordkeeping and off-channel communication

Global Relay's Industry Insights: Compliant Communications 2023 Report asked respondents whether they were anticipating that U.K. regulators would be next to enforce against recordkeeping non-compliance. After almost two years of sustained enforcement activity from U.S. regulators, *CityAM* had reported that the FCA was "actively discussing personal device use with a range of U.K. authorized firms" in light of regulatory action in the U.S..

38.5% of respondents said that they were anticipating action and taking proactive steps, while 10.3% said that they were worried as U.K. regulators may be next to act, and they weren't prepared.

Enforcement action from unlikely regulators

In April 2023, shortly after our 2023 Report was published, U.K. energy regulator Ofgem issued a £5.4 million fine to Morgan Stanley & Co. International for recordkeeping failures. Ofgem found that, between January 2018 and March 2020, Morgan Stanley had failed to record and retain electronic communications relating to wholesale energy product trading.

In particular, many of these exchanges had taken place via private WhatsApp conversations, contrary to Morgan Stanley's policies.

Also in April 2023, the Prudential Regulation Authority (PRA) censured Wyelands Bank Plc for its failure to retain WhatsApp messages.

While survey respondents were right to have worried that U.K. regulators would be next to act for non-capture of WhatsApp, they likely did not expect that the PRA or the energy regulator would be leading the charge.

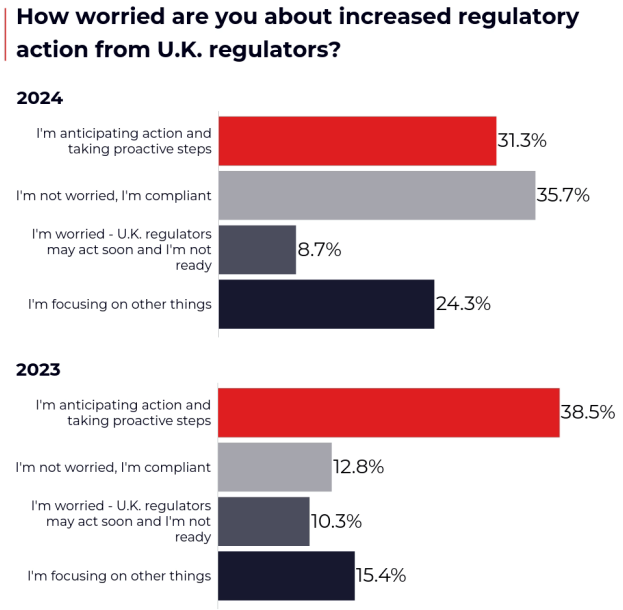
Will the FCA be next to act?

Speaking at Global Relay's offices in February 2024, the FCA's Head of Secondary Market Oversight, Jamie Bell, sought to level the debate by suggesting the FCA would not take a hard-line approach akin to that of its U.S. counterparts, and that instead it wants to see robust policies that are adhered to. In May 2024, Thomson Reuters reported that a Freedom of Information request uncovered that the FCA has opened no investigations into recordkeeping compliance between 2020 and 2023.

Despite warnings from the U.K. regulator that there is "nowhere to hide" for non-compliance, and for organizations to get their "ducks in a row now," the extent to which U.K. firms are concerned about regulatory action for recordkeeping has understandably diminished.

In 2024, 31.3% of U.K.-based respondents have said they are anticipating action and taking proactive steps, a decrease of 7.2% year-on-year (YoY). Notably, the number of respondents opining that they are not worried because they are compliant has risen by 22.9%, from 12.8% in 2023 to 35.7% in 2024.

Similarly, the FCA has highlighted several priority areas for 2024, including non-financial misconduct, insider dealing, and consumer protection – which may mean recordkeeping fines are off the cards, for now. However, it is still likely that FCA examinations will ask questions about how firms are achieving full recordkeeping and monitoring compliance of relevant communications.



Martin Gaterell, Associate Director: Private Side Advisory with Monitoring & Surveillance, Unicredit GmbH

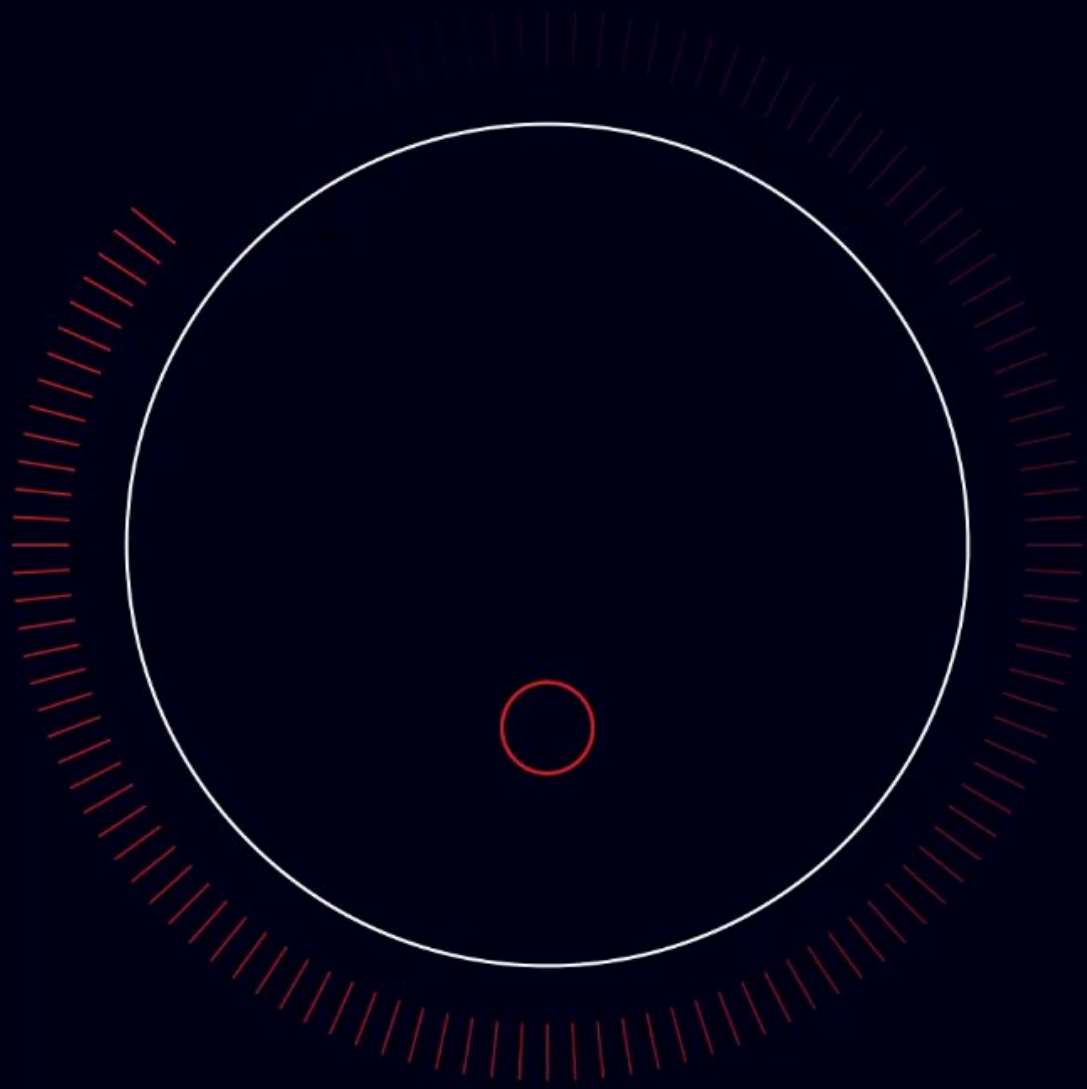
I think ‘not worried’ may be bravado or group speak when in reality, it is at best a case of ‘less worried!’

One has to question whether this is driven by the relatively low number of fines in the U.K. due to eComms surveillance failures. One is never at a stage when one is NOT worried about compliance and the regulators, that is the lot of a compliance officer. What we see against this result is a combination of the two key answers, a coming together of clear regulatory expectation which the vendor community has responded to. However, I think the compliance environment is now mature and despite being under constant forward momentum, it has a very clear understanding around the level of expectation from the U.K. regulator.

Regardless of the size, complexity, or nature of your business, I think the industry really does know what they need to be ready to deliver, even in the most rudimentary form. With various Market Watch notices, we have been advised about the expectation of not just operating ‘out of the box’ systems and it would be hard to say, “we didn’t know.” Ignorance will be no defense, as it has never been. The tools are more effective now and despite the warning from the regulator, even an ‘out the box’ solution will provide a company with a sufficient level of comfort.

Social media as a compliance risk

Is social media a compliance risk, and how is that risk being managed?



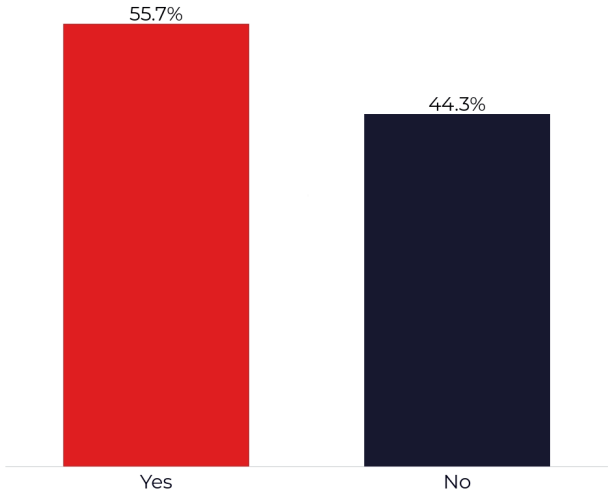
The hidden risks of social media

Global Relay's Data Insights Report 2023 referenced the data of over 10,000 financial services firms to analyze which communication channels are most commonly captured for compliance. In comparison to "traditional" business communications channels, such as email, SMS, and financial messaging tools, it became apparent that social media was being increasingly considered as a compliance risk.

> In particular, LinkedIn featured in the top three most captured communication channels, with 33% of financial services firms capturing LinkedIn communication data.

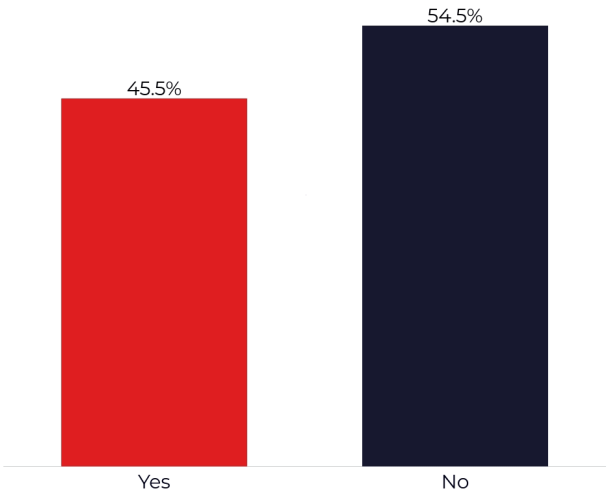
Social media poses myriad compliance challenges. The collapse of Silicon Valley Bank in 2022 was accelerated by panic on social media that saw backers remove their funding, hastening the bank's failure – dubbed the first ever "Twitter-fueled bank run." In January 2024, the U.S. saw billion-dollar market swings as a result of an SEC X account hack. As well as this, social media presents significant Marketing Rule and advertising risks, and provides yet more channels for potential off-channel communications.

Are you considering social media as a communication risk for your business?

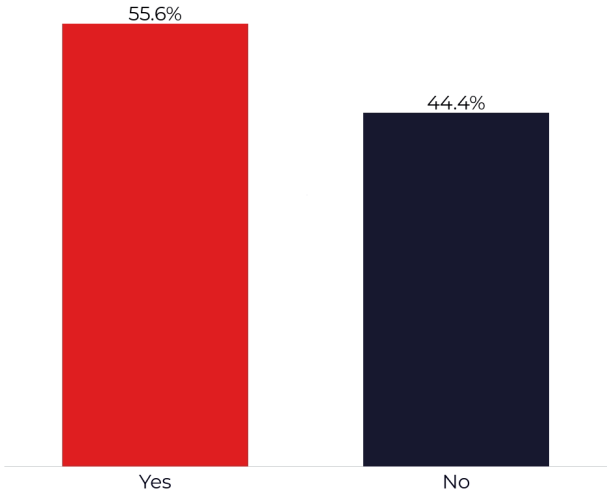


The risks of social media have not gone unnoticed in 2024's Industry Insights Report, with 55.7% of survey respondents noting that they are considering social media as a compliance risk to their business.

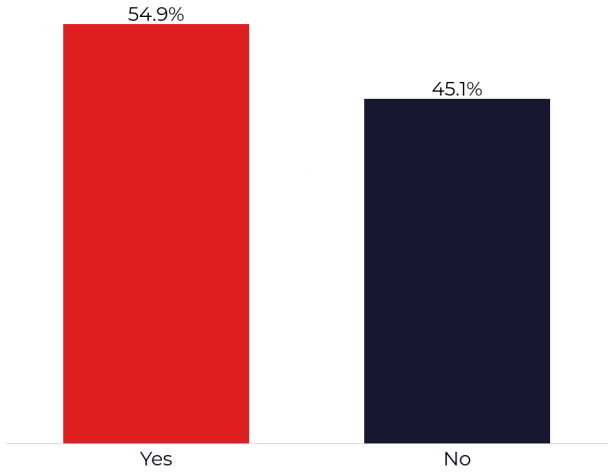
EMEA: Are you considering social media as a communication risk for your business?



Global: Are you considering social media as a communication risk for your business?



North America: Are you considering social media as a communication risk for your business?



When broken down regionally, both global banks (55.6%) and North American banks (54.9%) were slightly more cognizant of the risks social media presents. EMEA-based firms tilted the balance (45.5%) but, generally speaking, around half of all respondents see social media communication as some form of challenge for compliance teams.

5 main approaches to social media as a risk

An analysis of the commentary offered by respondents around social media risk uncovered five main approaches.

1

Those who view social media as a Marketing Rule or advertising risk

"As a private equity firm, we offer our funds privately. Therefore, no advertising is allowed on public sites."

"Our business model does not include sales, policies prohibit use of social media for business and are monitored by Compliance."

2

Those who see it as a recordkeeping or communication risk, and are proactively archiving or monitoring

"We only allow LinkedIn, capture it on Global Relay, and pre-approve postings."

"We use lexicons to search for social media being mentioned in email, and then have approved social media platforms."

"Compliance approval of social media and compliance monitoring by periodically logging in to see what communication, if any, there is."

"Use of LinkedIn for staff who opted-in for archiving."

3

Those who perceive it as a risk, but are uncertain of a watertight solution

“We don't allow the use of Instagram, TikTok or Snapchat, but we also don't have a way to monitor them to be sure they aren't being used – other than doing a Google search and using lexicons in our email monitoring.”

“These are banned, but it's impossible to put a perfect control in place to enforce.”

“We are trying to sort out how to archive and keep costs down.”

4

Those that manage social media channels through policies

“We have a social media policy banning the use for business communications.”

“The firm is constantly updating its social media policies around communications and the tools allowed for business.”

5

Those that have banned it altogether

“We do not allow social media usage.”

“We block access to social media sites from our corporate network.”

Solving social media

The main challenge posed by social media is that the proliferation of its use within a business context has been gradual and is, as yet, still an emerging risk. Social media, especially channels such as LinkedIn, blur the line between personal communication and business communication which poses distinct recordkeeping challenges.

Carroll Barry-Walsh, Lawyer, Speaker, and Founder at Barry-Walsh Associates

> **Social media is a real nightmare for compliance. Again, companies risk tying themselves up in knots by sending out mixed messages. It's the problem with telling staff to 'bring their whole self to work.' This blurs the boundary between your professional self – which is what you should bring to work – and your personal self, which is not anyone's business but your own and which keeping separate from your work life is probably necessary to stay sane.**

Employers need to guard against behaving like a mother, monitoring and tut-tutting about every aspect of their employees' lives. They also need to guard against imposing a 'received opinion' on everyone, especially about non-work topics expressed outside work. So, firms need to be clear – if they monitor social media channels – what exactly are the compliance risks they are looking for. Make these clear to staff so that they understand the boundaries. Firms also need to make a distinction between stuff said, which could be attributable to the firm (especially if the individual is senior), and stuff said in a personal capacity.

If it's just 'things we don't like to hear or disagree with' or they are making it up as they go along, they risk getting in a legal mess. A certain amount of toughness is needed: companies and staff should not allow themselves to be bullied by social media activists or trolls.

Without individuals having clearly separated personal and business accounts, it is difficult to know how to capture and monitor business communication data, without simultaneously capturing personal data which organizations may have no legitimate right (or interest) in capturing – and may be subject to stringent data control and anonymity requirements in some jurisdictions.

From a Marketing Rule or advertising perspective, social media presents similarly unchartered waters. In May 2024, the FCA brought charges against nine individuals who promoted an unauthorized foreign exchange scheme on social media.

In the U.S., FINRA fined a firm $850,000 for social media posts made by “finfluencers” on the firm’s behalf, which were found to be misleading. Similarly, the SEC’s Marketing Rule 206(4)-1 imposes strict limitations on how firms can market their products, which extends to social media.

Rob Mason, Director of Regulatory Intelligence, Global Relay

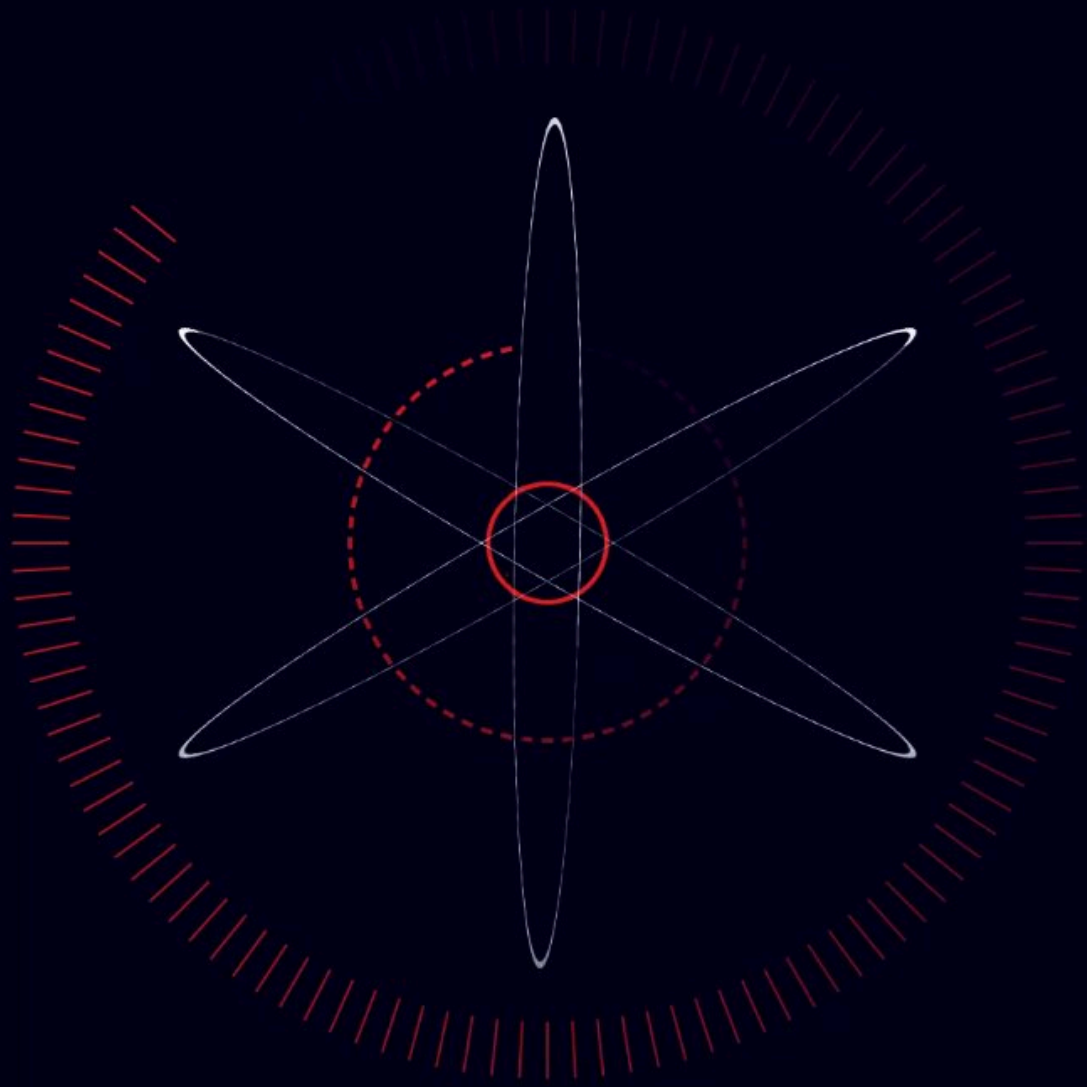
> **Finfluencers is another focus area where we have seen regulators trying to take a strong stance.**

Those who benefit from ‘stock-tipping’ without declaring their beneficial interest are in the regulators’ sights, but the ability to reach a wide number of followers means that the influence of some on financial markets and regulated securities can be huge. As we have seen with Elon Musk, it doesn’t take much to have a material impact.

Finfluencers can also perpetrate more fraudulent type activities, where the individual indirectly benefits from recommending followers invest in certain areas.

Artificial intelligence as a risk or a reward for compliance

How are businesses approaching AI in compliance now, and in the future?



The rapid evolution of artificial intelligence

Artificial intelligence (AI) has long been on the compliance agenda. The launch of ChatGPT in November 2022, followed by other significant generative AI platforms built on top of large language models (LLM), saw mass accessibility for AI, both for compliance teams and individuals within organizations.

2023 was a year of reckoning for AI and generative AI, with regulators, governments, and financial institutions attempting to assess its merit and develop guardrails. Many financial organizations initially sought to ban ChatGPT, with Bill Gates declaring it "the most important advance in technology since the graphical user interface." X founder Elon Musk called for an "immediate pause" to training generative AI, while some technology and compliance vendors rushed to integrate it into their technological offering.

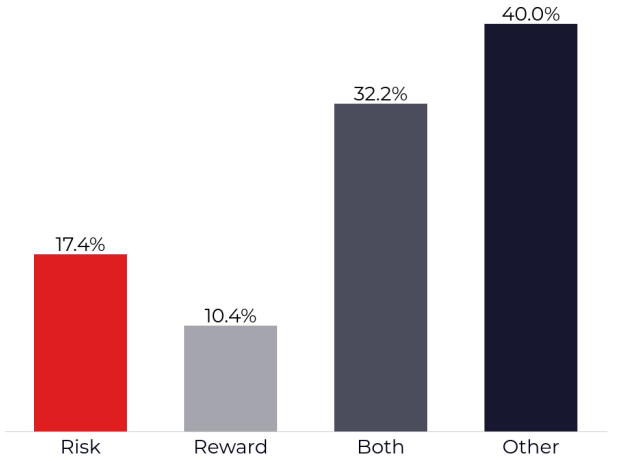
Is artificial intelligence a risk, reward, or both?

Regulators are progressively creating legislation or guidance regarding compliant approaches. With this in mind, this year we asked respondents their sentiments regarding AI and compliance.

Only 10.4% of respondents categorically assess artificial intelligence to be a reward for compliance teams, while 17.4% believe it to be a definite risk. 32.2% opined that AI offers both risk and reward, while 40% of respondents chose instead to tell us their opinions on AI by selecting "Other."

21% of respondents who chose "Other" opined that it is too soon to make a decision about AI, or that they had no intention of engaging with it.

What is your attitude to artificial intelligence (AI) when it comes to compliance? Risk, reward, or a bit of both?



Robert Nowacki, Technical Account Manager & Communication Surveillance SME, Global Relay

“

There’s no doubt that AI does offer reward, but it’s not instant or an overnight thing.

The only way firms are going to see the reward of AI is where they focus on data as a first priority. Financial services’ data is often all over the place – there’s no structure to it, there’s no clarity – and firms won’t see good outcomes with AI unless they manage that data first. From conversations with various financial institutions, it became clear that unstructured data from multiple platforms is their main blocker for a successful AI implementation.

At Global Relay, we’ve spent years capturing and storing data, and structuring it so that it’s easy for firms to search and draw insights from. This means that when we introduce AI, it can very quickly return accurate results instead of reams of false positives.

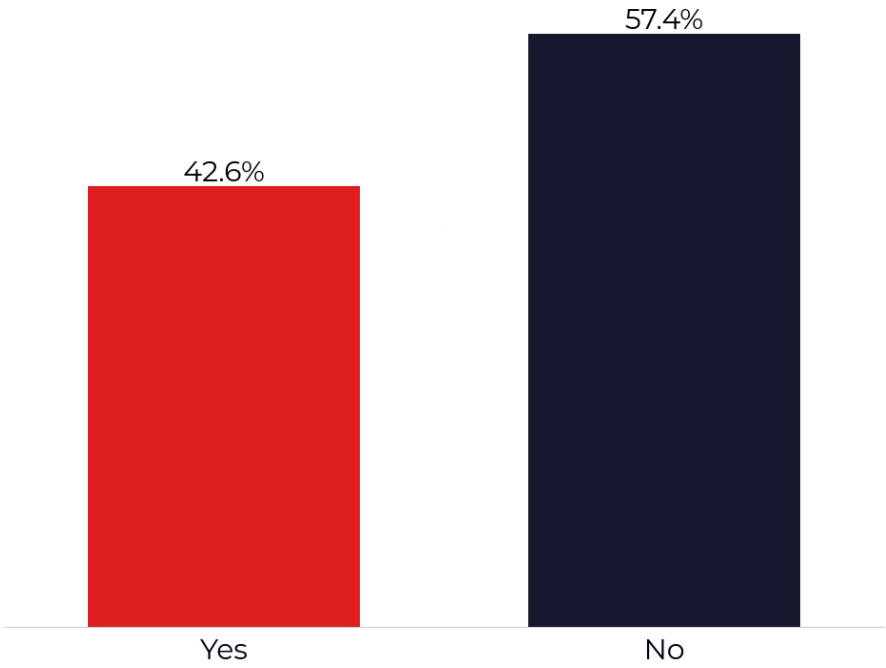
Firms can hire big teams of data scientists and AI professionals. But unless they start with data, and format it correctly, that would be wasted resource. If you want AI reward, invest the time into structuring your data first.

To better understand evolving approaches to AI, we asked respondents whether they intend to introduce AI into compliance workflows in the next 12 months.

While 42.6% of financial services said that they will be looking to integrate AI into compliance over the course of 2024, a greater number (57.4%) do not intend to.

These numbers provide further insight when broken down by regional respondents, as the figures are heavily skewed by an apparent reluctance to embrace AI by North American organizations.

If you're not using AI in your compliance workflow currently, do you intend to introduce it in the next 12 months?



Martin Gaterell, Associate Director: Private Side Advisory with Monitoring & Surveillance, Unicredit GmbH

The industry is waiting to fully embrace any solution that really and competently does provide a dramatic reduction of the industry problem across both trade and eComms surveillance, the false positive.

With the adoption of AI, one would expect to see an increase in regulatory expectation in terms of fewer, more precise alerts that in tandem will increase the amount of alerts to be properly investigated.

In more general terms, a harsh reality for many senior compliance officers is facing board-level colleagues and justifying what, on the superficial level, is little return on their equity or outlay and future demands for budget. Monthly MI can sometimes make bleak reading when one compares the number of alerts processed against any real or potential misdemeanors. Of course, we do not want to see large amounts of misdemeanors involving our own staff but sometimes management wants to see value for money.

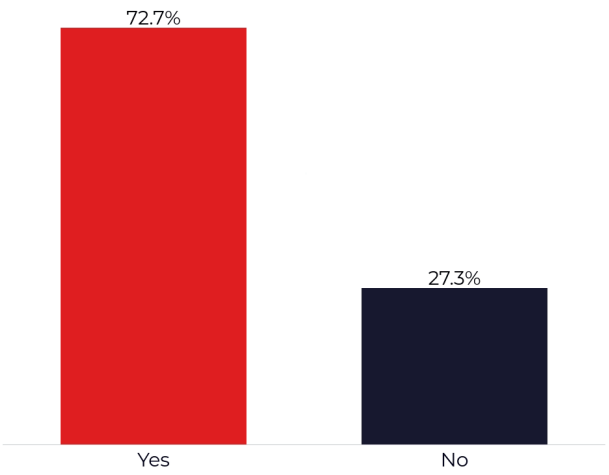
Why is it too soon? I think there are many societal considerations to be addressed before wholesale adoption in a rapid timeframe.

The banking sector is currently undertaking one of its periodical staff reduction phases coupled (again), with the talk of pan-European mergers of big banks which only adds to the job loss concerns.

The specter of AI adds to the social concerns of mass job losses, and this will provide a drag on rapid acceleration. There are also key privacy concerns to be addressed, be it basic rules around worker and client protection or use of information against clear boundaries. If AI will be as powerful and efficient as we are led to believe, then those clear boundaries have to be established and be strong.

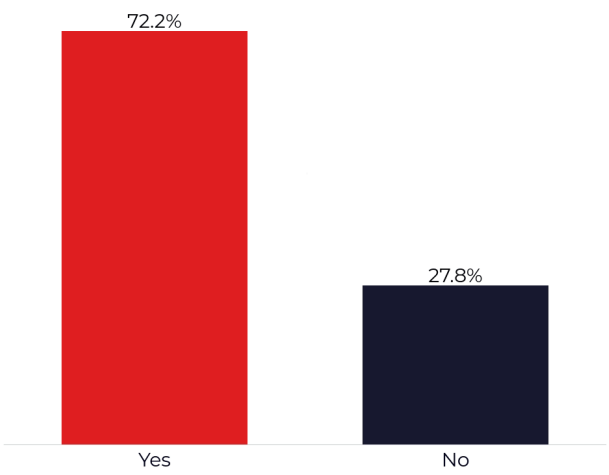
For compliance, the outcome will be good (eventually) but there will be cost. It will be slow creep until one organization goes ‘all in’ and succeeds in a 90% or more reduction in false positives, and gets better results with 90% less staff. At that point, the situation will change rapidly.

EMEA: If you're not using AI in your compliance workflow currently, do you intend to introduce it in the next 12 months?



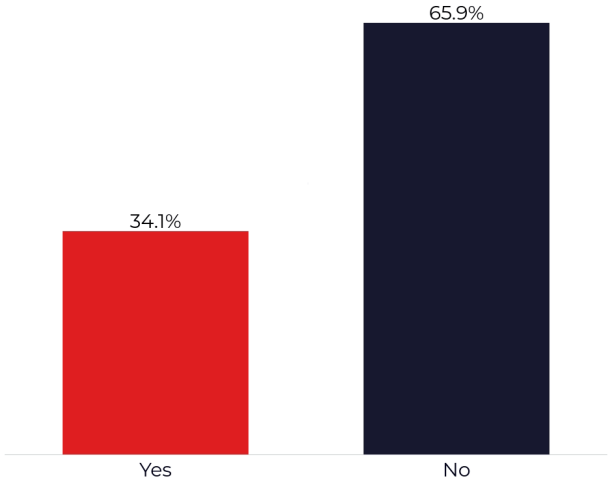
Roughly 70% of EMEA-based and global respondents expressed intent to integrate AI into their compliance workflows in the next 12 months.

Global: If you're not using AI in your compliance workflow currently, do you intend to introduce it in the next 12 months?



This encapsulates AI-driven tasks across the gamut of compliance: from more efficient alert management and regulatory change management, to AI-powered surveillance.

North America: If you're not using AI in your compliance workflow currently, do you intend to introduce it in the next 12 months?



North American respondents, on the other hand, show a markedly different attitude to AI adoption, with only 34.1% planning on integrating AI solutions through 2024.

Is North America against AI?

Clearly, U.S. financial organizations have reservations about introducing AI practices into sensitive, oftentimes vulnerable, compliance programs. This may in part be a trickle-down effect of a cautious approach from U.S. regulators.

Thus far, the regulatory approach in the U.S. has been measured and chiefly focused on risk. The CFTC, for instance, has declared it is “technology neutral” and focusing on AI evolution – particularly in relation to fairness, transparency, safety, security, and explainability. During the CFTC’s “AI Day,” the National Institute of Standards and Technology (NIST) Chief AI Advisor said:

> **In order to be able to improve the trustworthiness of the AI system – the safety, the security, and the privacy – you need to know what they are… and how to measure them.**
>
> **Chief AI Advisor, National Institute of Standards and Technology (NIST)**

SEC Chair Gary Gensler appears to have endorsed an :approach with caution" ethos, while the Biden-Harris administration has released an Executive Order on the use of AI to increase transparency and accountability related to the morphing technology, while laying the groundwork for defined governance. While all approaches focus on risk, there is not yet one unified message or clarity of approach.

In comparison, regulators across EMEA are taking one of two approaches: tackling the issue head-on, as seen in Europe, or adopting the more relaxed line U.K. regulators seem to be taking.

Turning first to the U.K., Jamie Bell has said that the FCA aims to be “an enabler, not a blocker” to AI growth. The FCA’s latest AI Update noted that:

> **Many risks related to AI are not necessarily unique to AI itself and can therefore be mitigated within existing legislative and/or regulatory frameworks. Under our outcomes-based approach, we already have a number of frameworks in place which are relevant to firms’ safe use of AI.**
>
> **FCA**

The U.K. approach therefore appears to be a consideration of fitting new risk into existing regulation. Europe’s approach is far different. It has enacted landmark rules on artificial intelligence which will enter into force in June 2024. It might be the case that the clarity of approaches across EMEA, though different, contributes to an overall confidence in the implementation of AI. Whereas a lack of clear guidance and a cautious approach in North America may be setting the tone across the region.

Chip Jones, Executive Vice President, Compliance, Global Relay

The jury is still out in the U.S. regarding the efficacy of AI in financial services compliance. Before U.S. financial services firms fully embrace AI to assist with compliance, these firms will need to see definitive data that demonstrates that AI is in fact assisting in reducing the compliance burden.

These firms are also waiting on clear direction from regulators (SEC, FINRA, etc.) regarding recordkeeping requirements if AI is utilized. Firms realize that if they use AI, they need to be able to explain to the regulators what goes on inside the AI algorithms.

Once U.S. financial services firms can clearly see the benefits of AI in the compliance space, and regulators have clarified recordkeeping and audit trail requirements, I think we will see adoption of AI in the U.S. financial services industry increase exponentially.

Industry insights

Is AI a risk or reward for compliance?

"AI could be a useful compliance monitoring tool. It is higher risk when deployed to investment professionals."

Chief Compliance Officer, Private Equity, North America

"I see that AI may help, however it is only as good as the information that it is provided. For instance, I may not be able to drill down into E.U. sanctions set in 1985 because the information has not been provided up through that year."

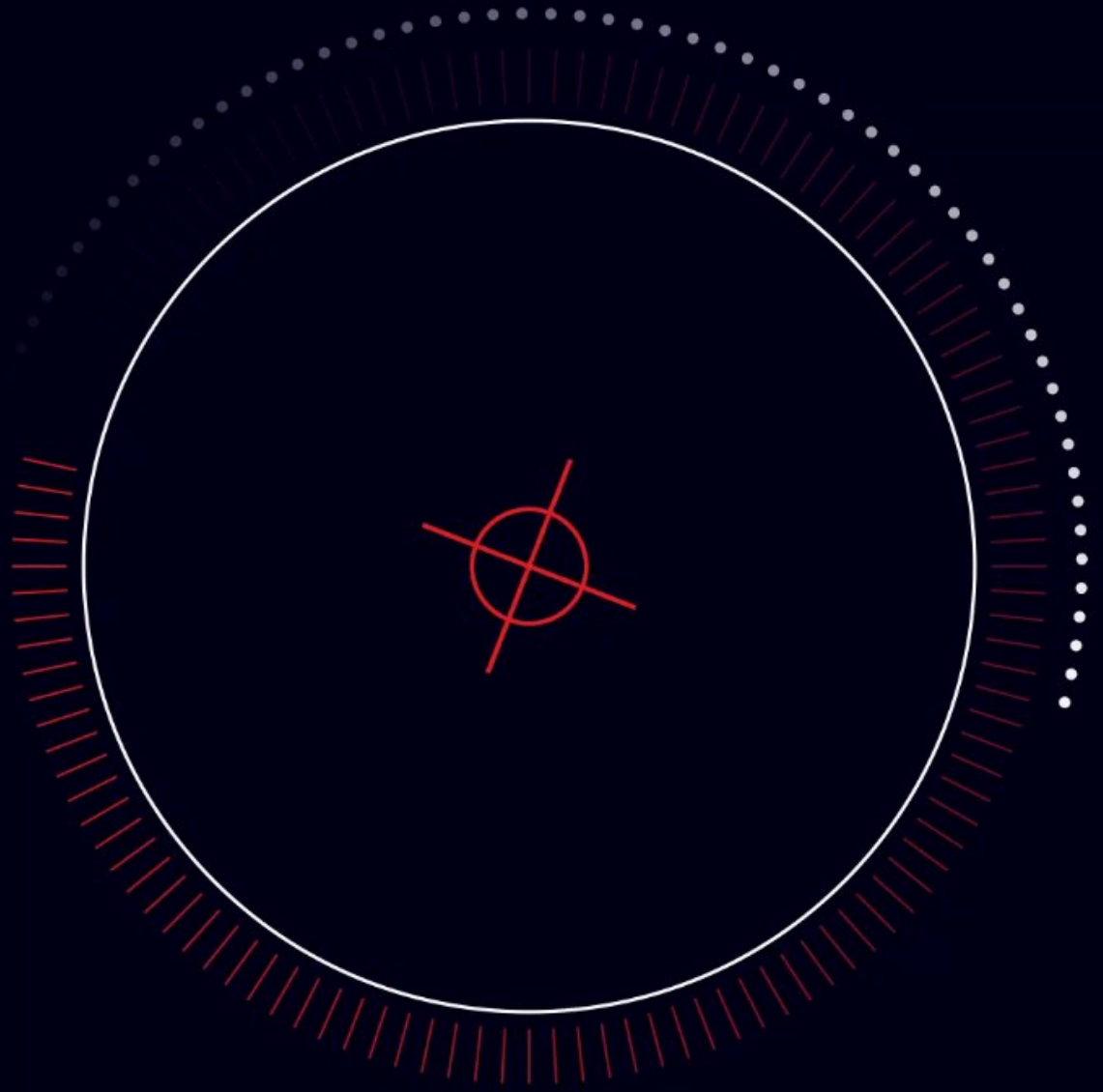
Registrations Compliance Manager, Investment Bank, Global

"It is inherently combined in so much of what we do already electronically that we have to make space for it. But be intelligent in our use and policy making surrounding it."

Senior Associate, Financial Services, North America

Surveillance as a solution to conduct and ethics risks

How are businesses using surveillance to tackle non-financial misconduct?



Non-financial misconduct and ethics – back on the regulatory agenda

In August 2023, U.S. regulators issued some of the most severe messaging yet around a “zero-tolerance” approach to a “culture of compliance,” driven partly by frustration around the lack of progress in controlling off-channel communications.

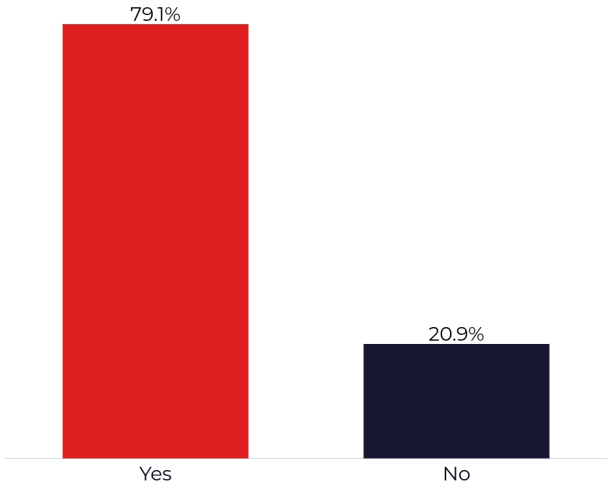
In February 2024, the FCA issued surveys to insurers and agents requesting data related to incidents of non-financial misconduct. In particular, the U.K. regulator requested information surrounding the number of non-financial misconduct incidents recorded, and the outcomes of those incidents, including bullying, sexual harassment, and discrimination.

Is communication surveillance the solution?

With this in mind, we asked respondents whether they are using communications surveillance to identify conduct and culture risks.

Almost 80% of respondents said that they are employing surveillance tools as a means to monitor bad culture. When split by jurisdiction, it is clear that this is much more prominent in global and North America-based firms.

Are you using communications surveillance to identify conduct and culture risks?



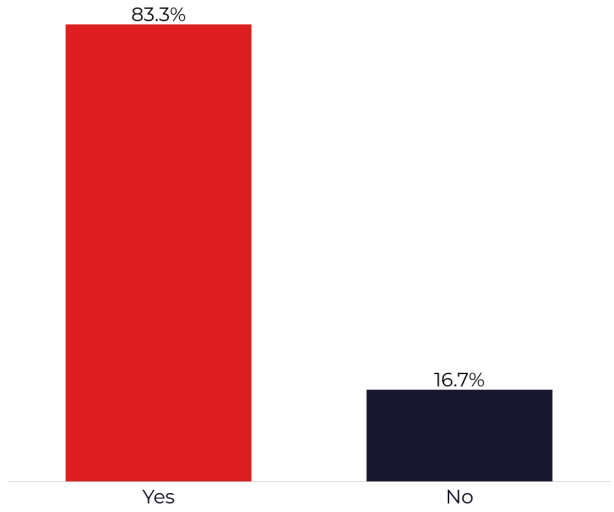
Emma Parry, Senior Advisor on conduct, culture, and risk

“There is an increasing realization in the industry of the need to be more predictive and proactive around misconduct and the role poor culture can play.

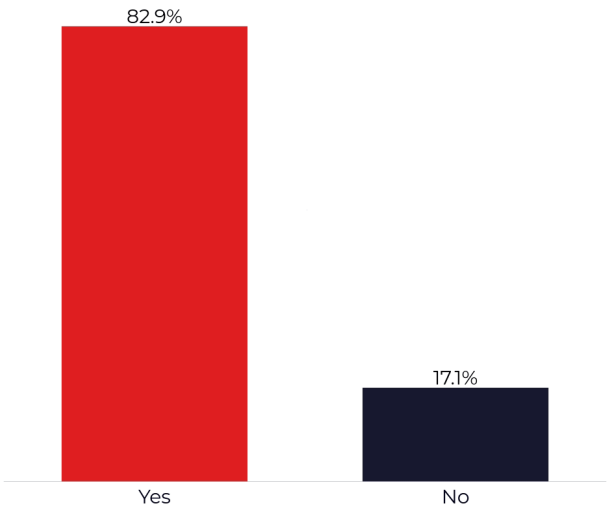
This is why we have witnessed the emergence of RegTech solutions underpinned by behavioral science and social network analysis. However, these come at a price – not just the cost of licenses and integration – but in terms of resources and ongoing capacity to analyze and assess the resultant data.

It is unsurprising therefore, that firms are increasingly leveraging their existing surveillance platforms – and teams – to pinpoint poor culture while also using the same platforms to monitor for potential market abuse and to support formal investigations.

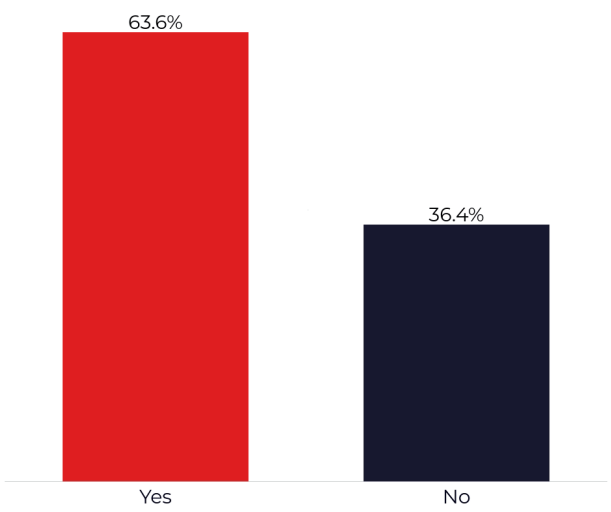
Global: Are you using communications surveillance to identify conduct and culture risks?



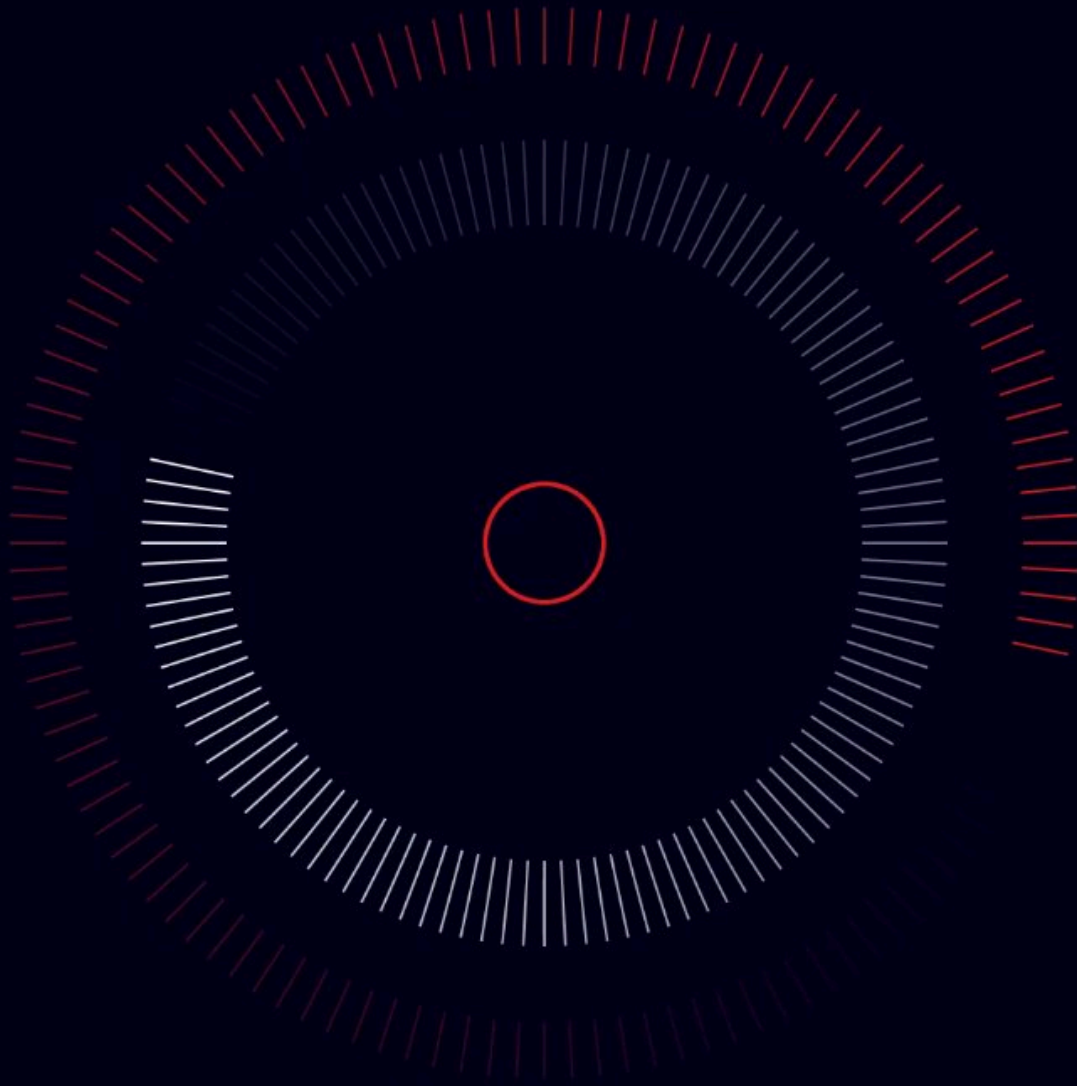
NA: Are you using communications surveillance to identify conduct and culture risks?



EMEA: Are you using communications surveillance to identify conduct and culture risks?



What does the future hold for compliant communications?

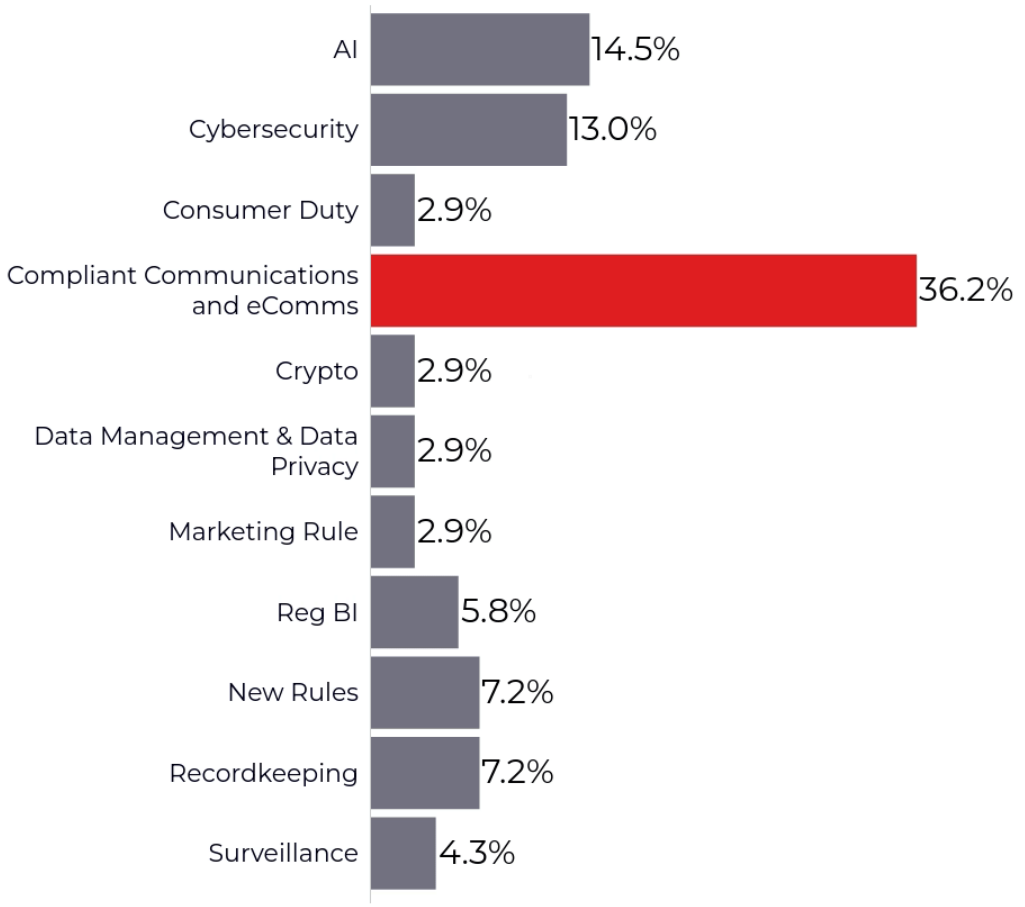


If the varied findings of this report have one thing in common, it's that there has been considerable change over the last 12 months. In some instances – AI, as an example – that change has happened fast. In other instances, such as the continued implementation of solutions for WhatsApp, that change has been more gradual.

Undoubtedly, change will continue to take place over the proceeding 12 months, especially given that 2024 will be a year of elections, further regulatory shifts, and likely the introduction of even more sophisticated ways to communicate.

We asked respondents what they expect the main area of regulatory focus to be over the next 12 months.

What do you expect to be the main area of regulatory focus over the next 12 months?



Are you communicating compliantly?

When asked what the main topics of regulatory focus for 2024 would be, 36.2% of respondents opined that compliant communications and eComms will likely be the main priorities for regulators. Other clear risk areas include AI and cybersecurity, which may form part of a wider operational resilience focus – an area some regulators are already increasing their messaging around.

Compliant communication and complete data sets underpin almost every facet of predicted regulatory expectation in 2024. Whether it's the monitoring of marketing communications issued for the purpose of meeting Marketing Rules, or capturing communications around the use of certain trading venues, as seen in a $350 million fine issued to JPMorgan Chase.

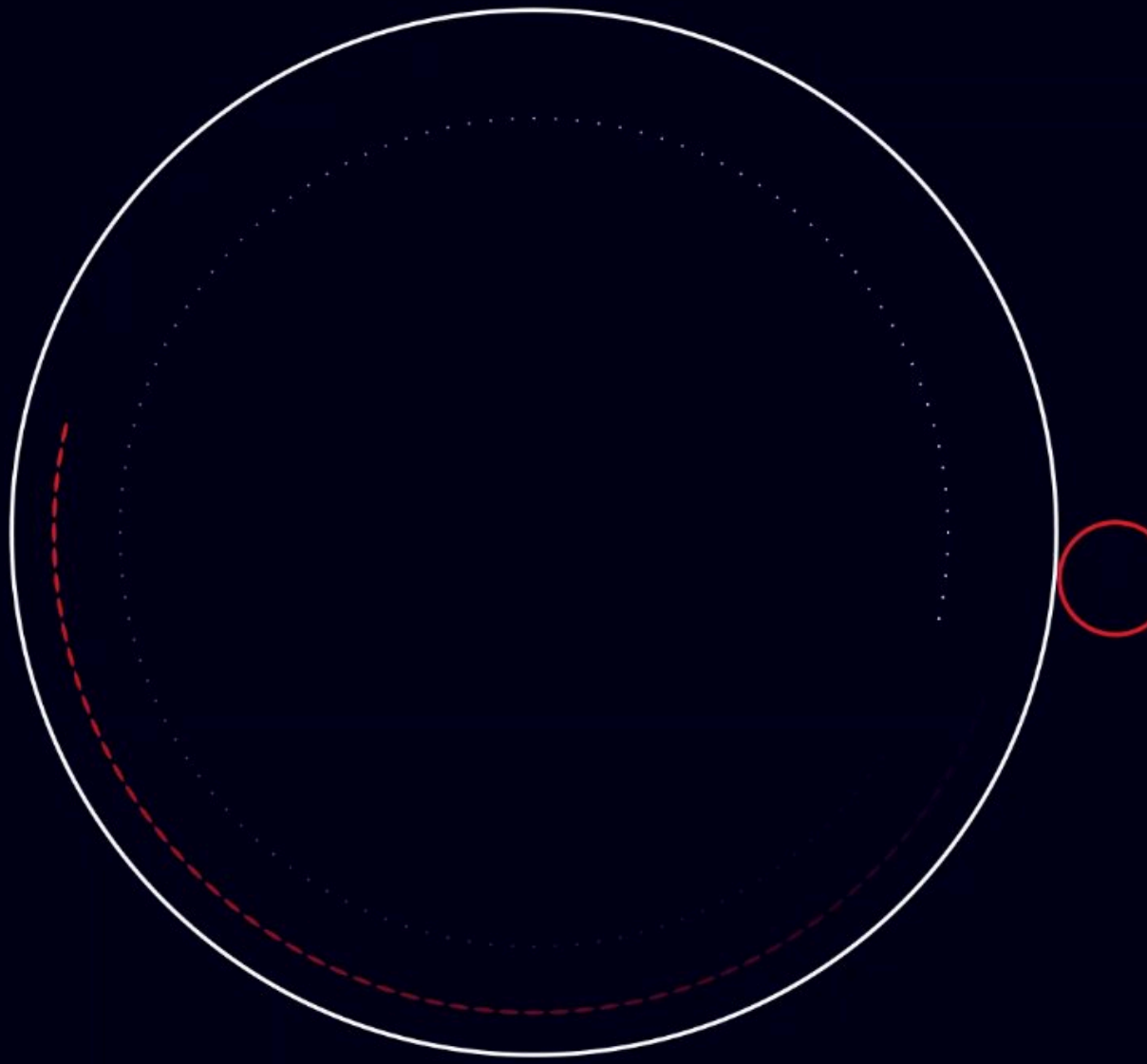
Complete, coherent, secure communication data (or lack thereof) is often at the core of regulatory enforcement action – bad data leads to bad outcomes. This is especially critical for AI, where the key to success ultimately lies in having clean, structured data to "feed the machine." Looking ahead at the next 12 months, it is likely that data will be the linchpin for compliance.

Whether, like 27% of survey respondents, you're struggling to capture business communication data, or whether you're joining 55% of respondents in their decision to ban certain communication channels, Global Relay has the solution.

From a collaborative messaging App to a trusted Archive, with a constantly evolving suite of data Connectors and AI-enabled Surveillance – Global Relay has the tools you need to communicate compliantly on any channel, from beginning to end.

FIND OUT MORE

Disclaimer



This report and the graphs therein refer to data collected by Global Relay Communications Inc. The information, materials, and opinions contained in this report are for general information purposes only, are not intended to constitute legal or other professional advice, and should not be relied on or treated as a substitute for specific advice relevant to particular circumstances.

Global Relay Communications Inc makes no warranties, representations, or undertakings about any of the content of this report (including, without limitation, any as to the quality, accuracy, completeness, or fitness for any particular purpose of such content), or any content of any other website referred to or accessed by hyperlinks through the report. Although we make reasonable efforts to update the information on our reports, we make no representations, warranties or guarantees, whether express or implied, that the content is accurate, complete, or up-to-date.

June 2024