NICE Actimize

FINANCIAL MARKETS COMPLIANCE

COMMUNICATIONS MONITORING REGULATORY PLAYBOOK

2 Billion Reasons to Ensure Communication Compliance

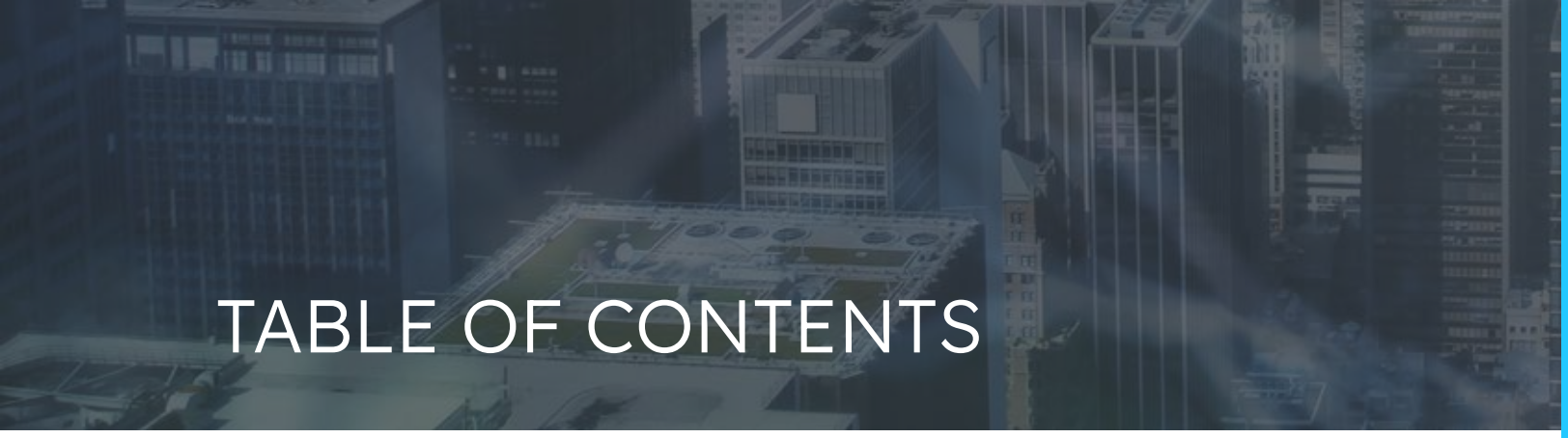


TABLE OF CONTENTS

REGULATORY ENFORCEMENT ACTIONS

Regulatory Fines

Since December 2021, twelve major U.S. and global investment banks have been fined for failing to properly record and retain employees' conversations with clients. Interestingly, several of the fines have been for similar aggregate amounts: USD $200 - $225 million for larger 'Tier One' banks, and $80 – $100 million for 'Tier Two' firms; these fines were split between the Securities and Exchange Commission (SEC) and the Commodities Futures Trading Commission (CFTC).

$200M here, $200M there, and soon you're talking real money (like, $2B). What are these banks doing wrong? In announcing the first fine last December, the SEC pointed to violations of books and records preservation requirements under the 1934 Securities and Exchange Act (specifically, Rules 17a-4(b)(4) and 17a-4(j)), and also to a failure of banks to reasonably supervise employees in order to detect or prevent further violations of these Rules. In its order, the CFTC cited violations of similar provisions under the Commodity Exchange Act (1936) related to record-keeping and supervision.

These SEC and CFTC Rules require U.S. banks and broker-dealers to capture and retain all business-related communications, including those related to sales and trading (regardless of how they are transmitted). Banks and broker-dealers must also furnish these communications to regulators on request.

There are three main reasons for imposing a recording requirement on communications related to transactions:

1. To ensure evidence exists to resolve disputes between firms and clients
2. To assist those empowered to supervise code of conduct adherence within the firm
3. To help deter market abuse through enhanced detection

Recent Case

In one recent case involving a bank that was fined $200M dollars, the firm's employees had communicated with clients over applications on their personal devices, which were not being channeled through the bank's systems, and therefore not being captured for preservation and potential surveillance. Because the records were not being captured and retained, they could not be furnished to the SEC upon request (if necessary). One inevitably leads to the other.

In addition to failing to capture, record and retain business-related communications made by employees, the bank also failed to take reasonable steps to ensure that staff was making business-related communications only over devices and applications which could be monitored and retained.

Taking Measures

One positive outcome of such fines, however, is that they provide ammunition to compliance departments to demand certain measures be taken. Among other things, these measures could include:

- **Banning business-related (or any) communications with clients** via non-approved channels
- Requiring that business-related communications take place **only over company-provided devices**
- Loading applications onto personal devices, which can then route communications on that device through company systems where they **can be captured and retained** (also known as 'bring-your-own-device', or BYOD).

The problem of business-related communications being conducted over personal or other non-monitored channels has been around as long as mobile phones. Having long ago identified this risk, many financial services firms banned the use of personal mobile telephones on their trading floors in the early-2000s. However, the problem went back further than that. After all, there was never anything physically stopping a banker from speaking with a client over his or her fixed-line home phone.

Increasing Number of Communication Channels

Whatever the case, the problem has snowballed in recent years. Fines have accelerated, and the number of choices regulated employees have for communicating has grown. Beyond simple SMS-based texting and email applications, employees have access to a variety of mobile instant-messaging applications that have come into popularity in recent years, including

- Messenger (released in 2008),
- WhatsApp (2009),
- Viber (2010),
- Snapchat (2011),
- WeChat (2011),
- Telegram (2013),
- Slack (2013) and
- Signal (2014).

And more entrants in the space are appearing and disappearing all of the time.

Many of these apps have end-to-end encryption capabilities, making these platforms attractive to bad actors who *want* their communications to be untraceable. This is exactly why regulators want all business-related communications to be carried out across compliant channels.

RECORD-KEEPING GAPS EXPOSED

Are firms asleep at the wheel? Yes and no. Historically, with regulated users working in the office, most business-related communications were conducted on a bank's premises where personal mobile devices were banned. Because of this, communications naturally tended to take place over established and compliant infrastructure, making this problem much more infrequent.

This cozy regime might have continued, had the status quo not been upended in early 2020 with the onset of the Coronavirus pandemic and the widespread (and rapid) transition to working from home.

At that time, many financial firms were logistically unable to deploy recorded-line infrastructure to their in-scope employees, meaning that in many cases, there was little alternative to using personal devices for work communications in order to keep business going. Many regulators recognized this, and for a time, permitted handwritten records of transactions to be made, subject to certain requirements.

However, it was clear that regulators would at some point be looking to ensure that proper records were being kept; for example, the UK's FCA clearly called time on its forbearance in January 2021, with the publication of Market Watch 66. One might easily conclude that when the regulators eventually did come knocking, they found more than they expected.

The fines to date do not suggest widespread deliberate conspiracies manufactured to intentionally hide business communications from employers or regulators. On the contrary, the SEC makes clear that in several recent investigations, numerous bank employees have co-operatively provided communications from non-approved and unrecorded channels on their personal devices (which is one way this problem came to light). Because of this, it appears that most in-scope staff – across all levels of seniority – simply didn't realize there was a problem.

Recording needed

That said, the CFTC has been clear that in several instances, senior employees not only knew they were doing the wrong thing by using non-permitted (unrecorded) channels, but encouraged junior staff to use these channels as well. Hence 'the tone from the top' was all wrong, and one CFTC Commissioner is clear that the tone for good culture emanates from the C-suite.

Transitioning to new work environments under COVID exposed pain points for all firms that were under a requirement to record communications. While these rules have long been set, it's now clear that all devices and channels used for business-related communications must be recorded and that the SEC and CFTC will impose penalties in the absence of proper record-keeping. And with 60% of firms not yet monitoring newer channels such as Microsoft Teams, Bloomberg, WhatsApp, Slack, Telegram and Signal , according to a NICE Actimize Survey, the likelihood that firms will be fined for not properly recording and retaining regulated employee communications has increased exponentially.

Moreover, it can be assumed that (to the extent it wasn't already) examining communications infrastructure and recordings will be on regulators' standard checklists for examinations and investigations.

60% of firms are not yet monitoring newer channels such as Microsoft Teams, Bloomberg, WhatsApp, Slack, Telegram and Signal.

THE PLAYBOOK: STRATEGIES FOR ENSURING COMPLIANCE

What do firms need to do to ensure compliance?

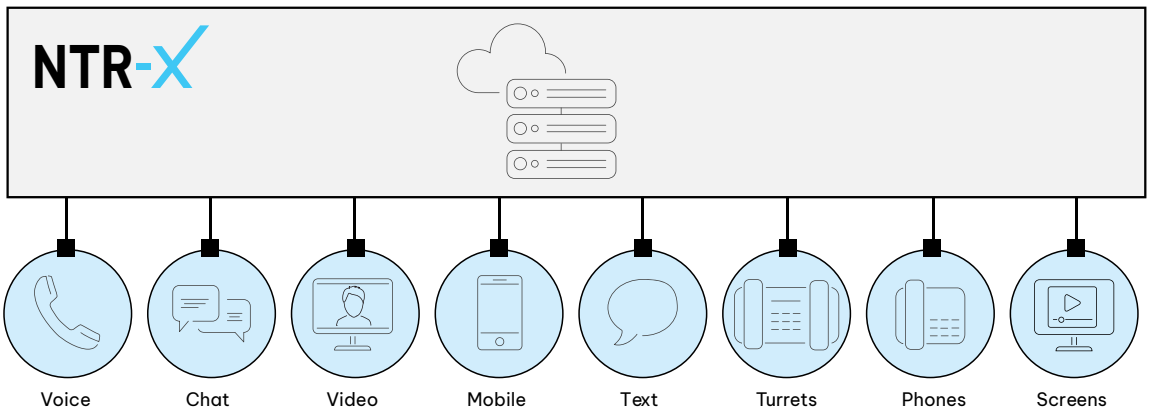
Capture All Communications in a Single Platform

Heads of Trading, Compliance and Operations are looking for ways to tackle this problem head-on by either issuing mobile devices that employees can use for business-related communications or installing communications monitoring apps on employees' BYOD handsets.

When it comes to recording these communications, firms are increasingly switching to **NTR-X** – the next generation of communication recording and assurance.

NTR-X provides one system to record and manage all communications. It adapts to all of the different ways your regulated employees communicate, whether they're using unified communications platforms (like Microsoft Teams, Zoom, Symphony), IPC Unigy or other turrets, Cloud9, mobile phones or PBX (desktop phones).

Additionally, **NTR-X** ensures seamless recording, archiving and retention of regulated employee communications, irrespective of where employees are working or the devices/modalities they're using to communicate. With one solution for every compliance recording need, your firm can keep overhead costs low and confidently comply with all global regulations around record keeping, and retention.



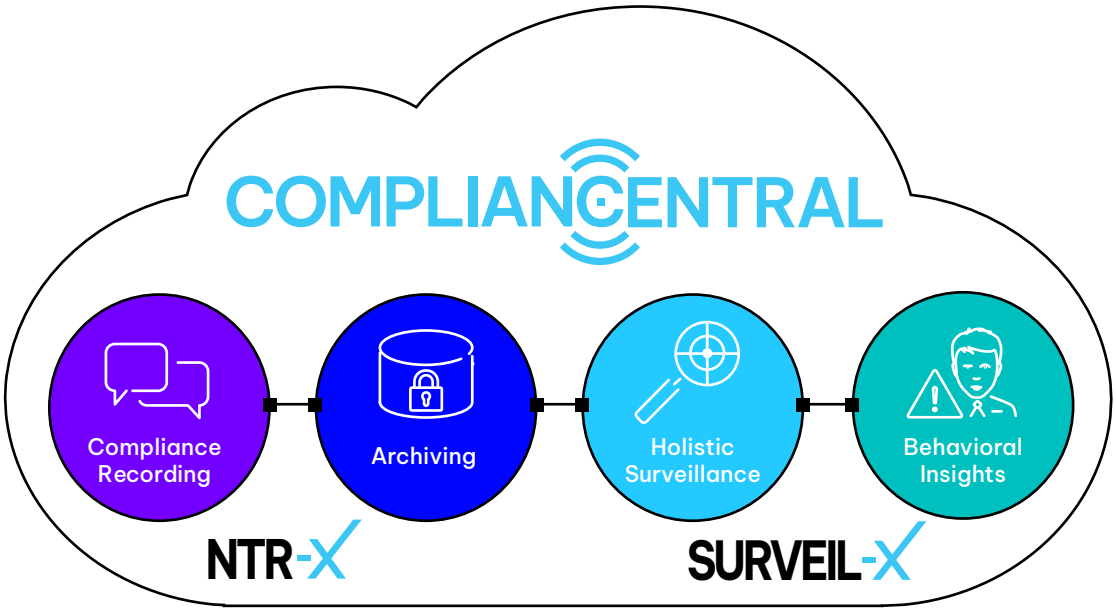
Proactively Monitor for Market Abuse and Conduct Risk

However, capturing and retaining relevant communications is only the first step. Regulators also expect these communications to be monitored, so that potential wrongdoing can be uncovered.

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

Using advanced analytics and AI (including Natural Language Understanding), **Compliancentral** can accurately detect all types of market abuse and conduct risk, by monitoring regulated employee communications across every communication channel, including turrets, desktop phones, mobile, email, instant messaging, chat, texts, social media, unified communications and even document attachments.

Compliancentral also uncovers hidden conduct risks by correlating employees' actions (trades and behavioral data) with their communications patterns and activities; the platform does this by merging trade communications and behavioral data into a single case management solution for more accurate and effective conduct risk monitoring and investigation. In the event that regulated employees try to get around monitored communication channels by switching to "offline" conversations, the system can also help detect this type of behavior.



Compliancentral is comprised of four integrated solutions:

- **Compliance Recording** – Capture all communications across all modalities
- **Archiving** – Retain all communications in a centralized platform
- **Holistic Surveillance** – Proactively detect all types of misconduct
- **Behavioral Insights** – Uncover hidden behavioral risks

CONCLUSION

Trust Depends on It

In financial compliance, trust is at the heart of everything you do. Market integrity and your firm's reputation depend on trust. Maintaining that trust depends on you. The problem is – risk can be hiding anywhere. Misconduct can lurk beneath the surface in millions of daily calls, emails and instant messages, in new communication channels used for hybrid work, and in growing trade volumes. Finding risk in this ocean of data is challenging.

With trust on the line, the fallout to your reputation and bottom line can be substantial. This is precisely where **Compliancentral** can help. **Compliancentral** shines the spotlight on misconduct, so you can know more and risk less.

Download the Compliancentral brochure

NICE Actimize

About Financial Markets Compliance

NICE Actimize Financial Markets Compliance is a leading compliance solution provider, serving more than 90 percent of the largest investment banks globally. NICE Actimize compliance solutions assist customers in the capture of trade conversations and trades, analyzing them for potential risk, and correlating trade conversations with trades for trade reconstruction.

The company's compliance solutions make automated and intelligent holistic trade compliance programs possible and enable FSOs to more efficiently comply with regulatory requirements, including MiFID II, MAR, FX Code of Conduct, Dodd-Frank and future directives.

niceactimize.com/compliance