# dubber

# How to comply with certainty

End not knowing

# Introduction

Compliance mandates are nothing new to financial services institutions and leaders in regulated industries.

Achieving compliance with a workforce based from home is the new challenge, causing many to rethink solutions that were quickly deployed as the pandemic impacted globally on workforces.

While initially regulators eased requirements to enable institutions to adjust to changing circumstances, many – such as the FCA in the UK – are once more enforcing the capture of conversations between bankers and customers, even if the banker is working from home. Leading institutions are looking to reduce the cost and complexity of compliance using a combination of people, process and technology.

This paper looks at how Unified Call Recording and voice data are central to meeting compliance mandates – from the practical answering of the need to record calls from anywhere, to knowing the customer through AI-enriched insights – and enabling continuous compliance through alerts and workflow automation.

Ending not knowing is the central tenet of continuous compliance.

# What's inside

# Why leaders are embracing UCR

The cost of not complying with call recording regulations is not only financial – it can be damaging for the brands of banks & financial institutions.

With home-workers utilizing mobile devices and a range of communications platforms such as Microsoft Teams and Cisco Webex, financial institutions face the challenge of ensuring that conversations taking place across every phone, PC or tablet are in compliance with monitoring requirements.

Call recording is no longer application or location specific and needs to be unified.

By capturing calls directly from the network with a Unified Call Recording (UCR) solution, firms can capture conversations from mobile devices across wireless and IP connections.

Shifting to a cloud solution frees financial institutions from the restrictions of application-specific and infrastructure-based call recording normally confined to call center environments. UCR offers a cloud-native solution that records directly from the network to complement remote working. Critically, UCR has minimal impact on user experience.

> "Without effective recording and monitoring controls, there is a real risk of loss of monitoring and surveillance capability, and the absence of protection through loss of evidence to resolve disputes between a firm and its clients over transaction terms. It is also vital to help with supervisory work, help deter and detect market abuse and to facilitate enforcement."
>
> *- FCA, 2021*

## A compliant Unified Call Recording (UCR) answers the need for:

### Recording of compliant and crucial conversations

From virtually any and every eligible end-point at a fraction of the cost of legacy hardware-centric and application specific approaches. UCR is a key component of effective monitoring for actual and intended market abuse

### Secure and compliant voice data management

With one unified repository of voice data that is protected for compliance purposes

### Legal Hold

Standard functionality that preserves important conversations for legal investigation

### Accelerated audits and investigations

Real-time search can retrieve any recording instantly

### PCI compliant call recording

With solutions to prevent the capture of sensitive information and meet PCI Data storage mandates

### Know your customer

Through keyword notifications, sentiment analysis and CRM integrations

### Recorded Voice Announcement (RVA) configuration

Announcements to let customers know the call is being recorded

### Recording & monitoring controls

Enable 100% compliance with policies and procedures

### Accurate record keeping

Accelerating dispute resolution and trade reconstructions with a unified data repository

# A checklist for achieving compliant conversations

We've identified key areas to achieve continuous compliance – whether your employees are texting, calling or messaging, no matter their location or network used.

## Can you compliantly capture all your conversations across dispersed end-points, platforms and networks?

Companies need to be able to meet all compliance requirements, even while employees are working from home. Financial authorities, such as the FCA in the UK, no longer provide any exceptions to bankers working remotely: all conversations must be captured. Traditional legacy and application-specific recording solutions don't address the complexity of today's workforce and communications. UCR offers a cloud-native solution that records directly from the network to complement remote working – operating independently to applications, with no impact on the customer or user.

## Can you compliantly store conversations?

UCR unifies conversational data in one secure and compliant platform. Deployed globally, the cloud platform allows data to be stored in the region of capture to ensure compliance with regional data sovereignty requirements.

When it comes to compliance, particularly in the financial services industry, storage needs to allow for retention periods of several years. Regulations such as MiFID II can require companies to store their recorded conversations for up to 7 years, or even longer. Your compliance solution must have the storage capacity to securely store recorded conversations long-term. Cloud storage has a significant advantage over on-premise storage, as data sets are protected with added geographic redundancy to meet data and privacy regulations.

### Are your recordings encrypted?

Captured conversations need to be protected. With conversations containing highly sensitive personal data, these recordings must be encrypted. And we don't just mean in storage. Data should be encrypted in transit with transport layer security, as well as at rest.

### Is your data protected by geographic redundancy?

To ensure stored data is fully protected, there should be redundancy measures in place to mitigate risk. On-premise solutions can't compete with the ability of cloud platforms to deploy across multiple data centers within a geographic region. Platform loads can be spread across data centers to provide full redundancy across all elements, including storage. Organizations need to prioritize solutions that serve all the major geographic regions, while ensuring the data is stored in a manner that reflects the compliance mandates applicable in those regions. Establishing a global standard saves time, money and management hassles, especially in the long run.

### Do you have a voice data retention policy in place?

Deleting data once it's no longer required is as equally important as storing it securely in the first place. Particularly when it comes to compliance with regulations like the GDPR. It's vital that organizations erase data when they no longer have a legitimate purpose to store it. Your solution should include the option to set retention periods for recordings so they are automatically deleted after a specified period.

## Are you prepared for a legal hold request?

Legal hold requests can happen at any time. These events mandate the preservation of information, including recorded calls and texts, and can cause hassle for businesses if their data isn't stored in a unified repository. To cover legal hold requests, your solution needs to have a feature to preserve recorded conversation to prevent deletion under any circumstances. This should override standard retention periods, the deletion of a user, or the expiration of overall storage periods.

## Who can access recordings?

Access to recorded conversations should be restricted to appropriate users for data protection, so your solution should enable strict and secure permissions and team structures. The solution should enable data permissions to be managed to prevent the deletion, downloading and sharing of calls, where applicable.

Make sure you can group users into teams and control who can listen to recordings within a team, such as only the compliance team. For best practice, users should only be able to access their own recordings and users outside a team shouldn't be able to access recordings.

To ensure data is transmitted securely, access to recorded conversations should be monitored and your solution should employ stringent password policies and granular permissions that control user access to system features, functionality, and recorded data. For extra security, access to content should be via tokenized sessions.

## Can you respond to regulatory requests in a timely fashion?

Regulatory requests and investigations need to be responded to in a timely fashion. Real-time search and discovery make this easy – providing instant access to data in order to comply with audits or other requests for information. All recorded calls should be instantly available to search, replay, securely download, review, or delete on request.

## Are your recordings capturing critical metadata?

Regulatory audits require a compliant data set to work from. As part of these procedures and others – such as legal hold requests or dispute resolution – organizations are often required to retrieve all calls from a specific time or date. Your recording solution should time-stamp all conversations and allow search results to be filtered by date or time as well as user. Call metadata such as call participants, recording name, and any tags should be stored alongside a recording, in addition to any AI information.

## Will you meet PCI DSS requirements?

Compliant call recording also needs to consider PCI DSS requirements. Some information can be stored and used, but sensitive information such as cardholder data cannot be recorded. Your call recording solution must have the ability to prevent the recording of this information: redaction is not enough. You should be able to choose the right PCI compliance solution to meet the needs of your business.

## Does your solution proactively mitigate risk?

Most industry regulations have been put into place in order to protect consumers and promote best practices. Your recording solution can actually be a useful tool for proactive improvements and risk mitigation when it includes voice AI. When calls are transcribed, keyword alerts can be put in place for the early detection of risky behaviour – deterring potential bad actors. When these words occur in a conversation, managers or supervisors will receive an alert with a link to the conversation in question.

## Does your solution help meet 'know your customer' (KYC) requirements?

Financial institutions must ensure that they know their customers and check that their funds come from a legal source. Your call recording solution should capture any confirmation of a customer's identity and the source of funds. Call metadata – including keywords and sentiment – should be used to enrich CRM records and generate customer-specific alerts.

## Does your solution provide RVAs?

Recorded voice announcements (RVAs) are played to both call parties on connection to notify participants that the call is being recorded. For compliance with regulations such as GDPR, parties must consent to the recording of their conversation.

## Can your compliant recording solution scale to meet demand?

To make sure you capture every single conversation, your recording solution will need to be scalable enough to cope with multiple concurrent recordings. Large multinational organizations may need to record thousands of conversations at once so your solution needs to ensure that all of these conversations are recorded.

## Can you implement Compliant workflows & rule-based automation?

Automation shouldn't stop at keyword alerts. To streamline processes within a business, your recording solution should include an open API that allows you to create intuitive workflows and rule-based automation. These can automatically populate other business applications for increased productivity and visibility across operations.

## Does your UCR solution deliver high-quality transcripts?

Most call recording solutions offer transcription. Look for solutions that provide flexibility in the transcription services provider and that are embedded in the service at no additional cost. Services offer varying degrees of language support. Critically, you should confirm that the transcripts are presented in a format that is readable for humans and machines alike.

## Does your UCR solution go beyond AI transcription?

AI and machine learning are used extensively to support transcription of speech to text. But does your UCR platform deliver AI as a critical solution feature – delivering, for instance, real-time alerts? Is the AI engine trainable to meet your specific business needs?

## Is your UCR platform purpose-built for compliance?

Most call recording solutions are built for customer sales and service in call centers. Compliance users have different requirements, ranging from the storage of protected data sets to investigative tools that accelerate processes such as trade reconstructions. Choose a solution with compliance features such as Legal Hold and unlimited storage as standard.

# Get started today!

Turning conversations critical data for compliance, business continuity, and productivity is imperative for enterprises.

Turning conversations critical data for compliance, business continuity, and productivity is imperative for enterprises. Capturing conversations directly from the service provider network and in collaboration applications, and aggregating that voice data with Unified Call Recording and voice AI is the answer.

Need help transforming your voice conversations into valuable data to meet compliance mandates, driver operational efficiency, improve service and sales performance, and reduce costs?

**Contact us today for a consultation with one of our voice data experts or visit dubber.net**

## Dubber is the world's #1 Unified Call Recording and voice AI solution for compliance and operational efficiency.

Dubber's fully compliant solution can be switched on with a click, and is infinitely scalable in the cloud – with no hardware requirements. Every conversation is captured automatically, stored securely in the cloud and available instantly to replay. Voice AI provides transcriptions, real-time search, sentiment analysis, alerts and more.

### HIPAA
HIPAA is United States legislation that provides data privacy and security provisions for safeguarding medical information, including protected health information. HIPAA distinguishes between two types of organizations: covered entities (physicians, hospitals and pharmacies), and business associates (claims processors, contact centers and third-party billing companies), both of which are required to comply with data protection regulations. Any recordings containing medical information must be kept secure and encrypted and should be securely stored for 6 years and beyond. Recordings need to be kept private with no unauthorized third-party access but must be available to replay at any time.

### GDPR
GDPR is an EU law, designed to protect the Personally Identifiable Information (PII) of European residents. Businesses that collect this information must gain consent to this data being recorded. Any personal information should only be stored for as long as it is required, and should be deleted as soon as it is no longer needed, and all access to data should be monitored to create an audit trail.

### PCI DSS
The Payment Card Industry Data Security Standard (PCI DSS) requires members, merchants, and service providers that store, process or transmit cardholder data to ensure they do not store security codes or PINs and only store primary account numbers or card expiration dates under defined encryption standards.

### Dodd-Frank
The Dodd-Frank Act was passed by the United States government to promote financial stability by improving accountability and transparency amongst financial service organizations. Dodd-Frank introduced extensive record-keeping regulations for the US financial services industry, including call recording requirements. Recordings must be stored for the lifetime of a transaction plus 5 years and must be readily accessible at the principal office of an organization. Call metadata, including call parties, date, and time must be accurate.

### MiFID II
MiFID II was put in place to regulate financial services organizations. This legislation impacts any company or individual offering financial advice who operate in EU countries. Calls containing financial advice must be recorded and securely stored for 5 or 7 years, depending on the country. Upon request, records and audit trails must be provided.

# Get started today!

**Dallas**

L12, Ste1200, 2828 N
Harwood Street, Dallas TX
75201, USA

**Atlanta**

F6, 3280 Peachtree Road,
Atlanta GA 30305, USA

**London**

8 Devonshire Square
Spitalfields, London
EC2M 4YJ, UK

**Melbourne**

L5-7, 2 Russell Street,
Melbourne, VIC 3000,
Australia

**Sydney**

L14, 50 Pitt Street
Sydney, NSW 2000,
Australia

**Brisbane**

L3, 293 Queen Street
Brisbane, QLD 4000,
Australia