HAYSTACK®

COMET™

Compliance Oversight for Mobile Electronic Transmissions

COLLECT IT. ARCHIVE IT. DEFEND IT.

Targeted, scheduled, recurring collection of business mobile communications, with privacy and GDPR designed in from day one. **Built for regulated financial firms and their compliance archives.**

COMET is a **targeted, scheduled, recurring collection** of business communications, NOT continuous capture. The distinction matters legally. In several jurisdictions, "continuous" capture can be classified as interception under wiretap or interception statutes (US 18 U.S.C. § 2511 and state two-party consent regimes, UK RIPA/Investigatory Powers Act 2016, EU ePrivacy Directive Article 5).

COMET acquires records from the device on a defensible scheduled cadence (forensic acquisition of stored communications), within a targeted scope (business communications, not personal), with **privacy and GDPR built into the architecture from day one**. It does not intercept communications in flight, it does not capture indiscriminately, and it does not treat personal communications as in scope.

WHO BUYS IT

- Chief Compliance Officer
- Head of Surveillance
- Head of Financial Crime and Money Laundering Reporting Officer
- Head of E-Comms Supervision

Not the litigator. Not the General Counsel. The compliance organization owns the budget, the relationship with the regulator, and the procurement cycle.

THE PROBLEM COMET SOLVES

WhatsApp, Signal, Telegram, and iMessage are how business gets done now, including the business that regulators care about. The record-keeping obligation has not moved. **The enforcement has caught up.**

FINRA, SEC, and CFTC have collected $3.5 billion in off-channel comms penalties since 2021. The FCA, BaFin, AMF, and ESMA are moving on the same theme.

MiFID II Article 16(7) and FCA SYSC 10A already require recording of all electronic communications related to order reception, transmission, and execution. The rules are not new. The audit posture is.

DORA (effective 2025-01-17) brings recordkeeping infrastructure into operational resilience expectations for European Union financial entities.

Most regulated firms address this by banning personal device messaging. That policy does not survive contact with reality. **COMET is the infrastructure assumption** that enables compliance to buy scheduled, recurring collection and retention without disrupting how the business runs.

Connect with HaystackID Experts 800.267.9695 | Info@HaystackID.com | HaystackID.com

WHAT COMET DOES

1. COLLECT
WhatsApp, iMessage, SMS, and MMS.

2. CONTROL
Scope, work-only split, opt-in, and termination.

3. RETAIN
Direct to your compliance archive. No lock-in.

4. AUDIT
Defensible audit trail. Role-based access.

DATA RESIDENCY
EU, UK, and US paths.

- **Targeted scope** by design: business communications only. Personal communications are not in scope. The work-only/personal split is a foundational assumption, not a configuration toggle.
- **Scheduled, recurring collection** across iOS and Android, currently covering WhatsApp, iMessage, SMS, and MMS. Signal and Telegram will soon follow (requires MEDAL Recon™ collection).
- **Retention** in the customer's nominated compliance archive (Global Relay, Smarsh, Theta Lake, Behavox class).
- **Direct integration** with those archives, not a parallel data store.
- **Custodian-level controls** for opt-in, scope definition, work-only/personal split enforcement, and termination workflows.
- **Defensible audit trail** at the collection, transit, archive, and access stages.
- **Privacy and GDPR were designed in from day one**, not retrofitted. Built for regulated employee monitoring under GDPR Article 5 minimization, Article 25 privacy by design, German works council law, French CNIL guidance, Italian Statuto dei Lavoratori Article 4, Spanish LOPDGDD, and UK employment regimes.
- **Region-scoped data residency** with EU and UK paths separated from the US path.

HOW COMET IS DIFFERENT FROM WHAT IS ALREADY ON THE SHELF

ARCHIVE-NATIVE

Sits with the archive, not in place of it. Theta Lake, Behavox, Shield, Relativity Trace, and Smarsh native each define a piece of the surveillance stack. COMET captures the mobile origin and directly retains it in whichever of those archives the customer already owns. No archive lock-in.

FORENSIC-GRADE CAPTURE

Forensic-grade capture, not consumer-grade MDM. Built and serviced by the same examiner bench that runs MEDAL™. The chain of custody supports both the regulatory enforcement record and the downstream litigation use of the same artifact.

PRIVACY BY ARCHITECTURE

Privacy posture is the architecture, not a setting. Work-only and personal-device splits, custodian-level retention windows, and data-residency choices are baked into the deployment model. EU buyers will not adopt a US-only collection tool that treats GDPR as a configuration toggle.

COMPLIANCE-TO-LITIGATION

Built for the compliance-to-litigation handoff. The records the CCO captures today become evidence in subsequent regulatory enforcement and civil litigation. COMET is designed to be defensible at both stops.

Connect with HaystackID Experts 800.267.9695 | Info@HaystackID.com | HaystackID.com