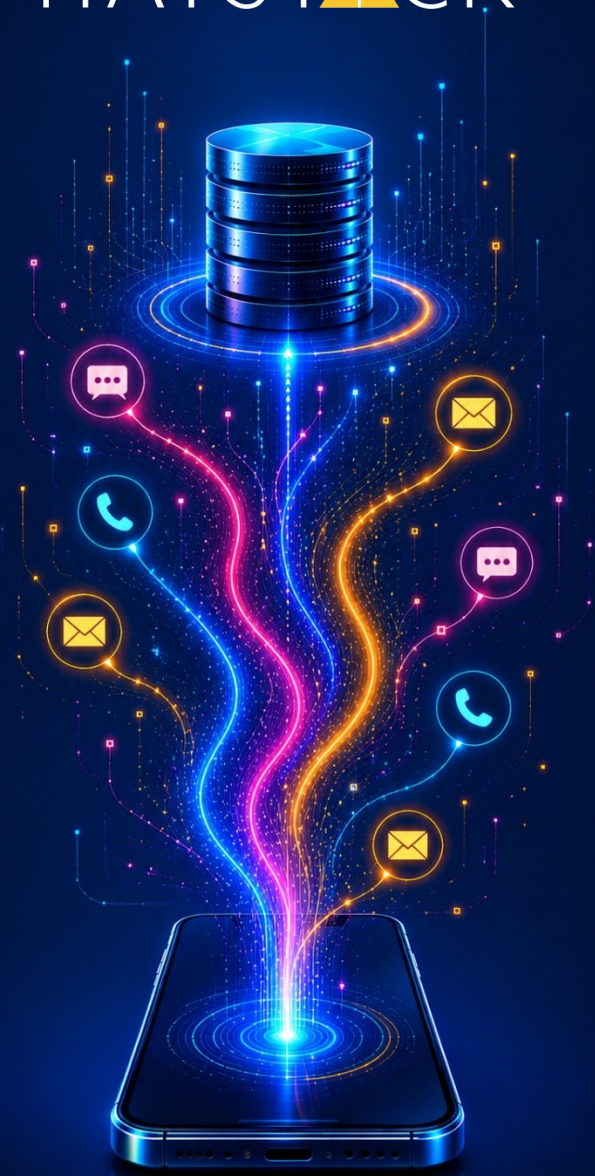


HAYSTACK[®]



COMET[™]

COMPLIANCE OVERSIGHT FOR
MOBILE ELECTRONIC TRANSMISSIONS

ILTACON

August 23-27, 2026

Meet Your Presenter



John Wilson

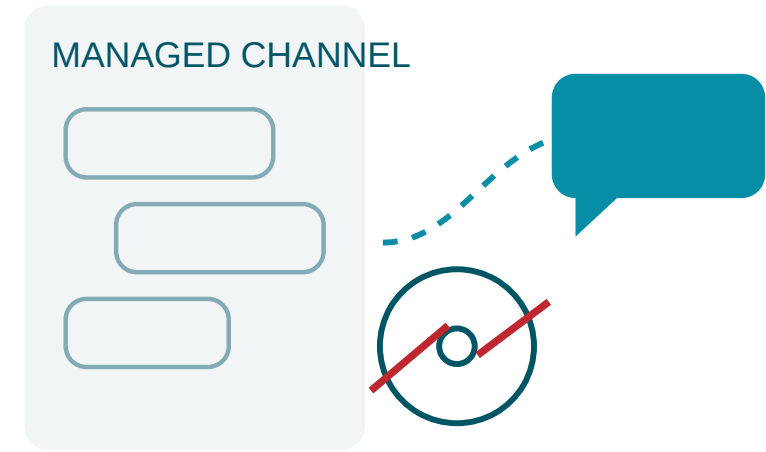
*Chief Information Security Officer and President of Forensics,
HaystackID*

As Chief Information Security Officer and President of Forensics at HaystackID, John Wilson provides consulting and forensic services to help companies address various matters related to electronic discovery and computer forensics, including leading forensic investigations, cryptocurrency investigations, and ensuring proper preservation of evidence items and the chain of custody. He regularly develops forensic workflows and processes for clients ranging from major financial institutions to governmental departments, including Fortune 500 companies and Am Law 100 law firms.

Why Now?

THE BUSINESS MOVED TO THE PHONE. THE RECORD-KEEPING DID NOT FOLLOW.

- ✓ WhatsApp, Signal, Telegram, and iMessage are how regulated business gets done now, including the business regulators care about.
- ✓ The recordkeeping rules have not moved. The enforcement has caught up to the channel.
- ✓ Most firms answer this by banning personal-device messaging. That policy does not survive contact with reality.



No usable record



WhatsApp



Signal



Telegram



iMessage

The Stakes

MORE THAN \$3 BILLION, AND THE THEME IS SPREADING.

\$3B+

Off-channel communications penalties collected from regulated firms since 2021.

FINRA, SEC, and CFTC off-channel recordkeeping actions since 2021; figure rounded, sources on file.

The FCA, BaFin, AMF, and ESMA are moving on the same theme.

The rule did not change. The phone did.

“

Regulators have collected more than \$3 billion since 2021 because firms could not produce the messages where the business happened. The rule did not change. The phone did. COMET captures that record before it becomes a fine.

John Wilson, Chief Information Security Officer and President of Forensics, HaystackID

What COMET Is

SCHEDULED, RECURRING COLLECTION OF BUSINESS MOBILE COMMUNICATIONS.



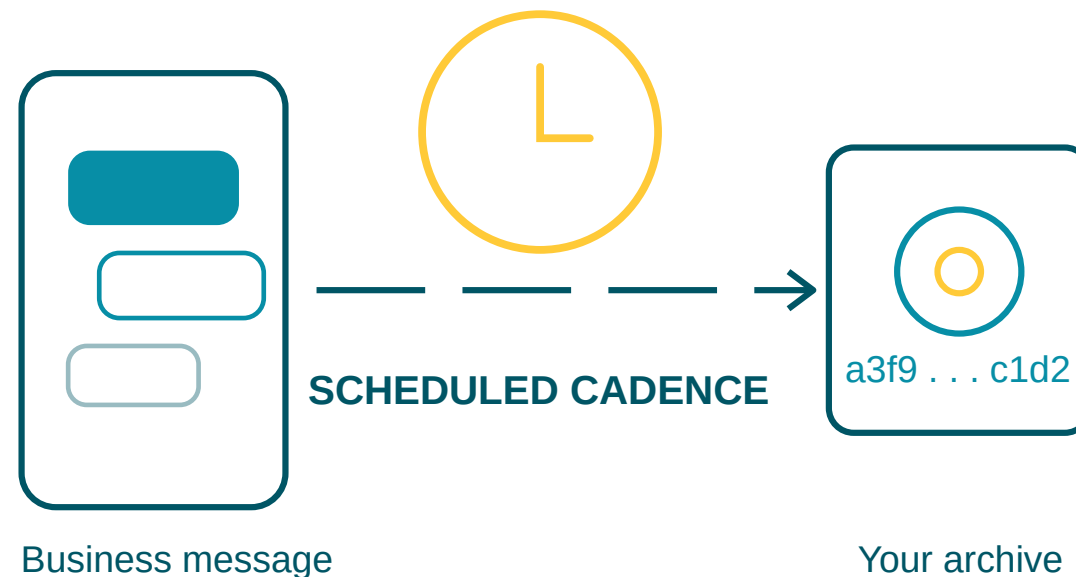
Targeted to business communications by design. Personal communications are not in scope.



Collected on a defensible, scheduled cadence, then retained in the compliance archive you already run.



Privacy and GDPR were designed in from day one, not retrofitted.



What COMET Does

COLLECT. RETAIN. PROVE. HAND OFF.



COLLECT

the business conversation
across the phone's
messaging channels, on a
scheduled cadence.



RETAIN

it directly in the
customer's nominated
compliance archive.



PROVE

it with a defensible audit
trail at collection, transit,
archive, and access.



HAND OFF

the record captured for
compliance today is the
exhibit that Legal relies on
later.

The Legal Line

SCHEDULED AND RECURRING, BY DESIGN.



Scheduled acquisition of stored communications.



Not interception in flight. Not indiscriminate capture.

COMET acquires stored communications on a defensible schedule. It does not intercept communications in flight, and it does not capture indiscriminately.

The distinction is load-bearing: interception in flight falls under wiretap and interception regimes; scheduled forensic acquisition does not.

“

COMET is a scheduled, recurring collection of business mobile communications, not continuous capture. The distinction is the whole point. UK RIPA and the EU ePrivacy Directive both gate continuous interception under regimes that place forensic acquisition outside. We built the product on the right side of that line by design.

John Wilson, Chief Information Security Officer and President of Forensics, HaystackID

Forensic-Grade, Not Consumer-Grade

A RECORD IS ONLY USEFUL IF IT HOLDS UP.



Sealed, hashed, chain of custody intact.

a3f9 . . . c1d2



A plain export, unverified.

No provenance to point at.

COMET is built and serviced by the same forensic bench behind MEDAL™, HaystackID's mobile forensic investigation suite, not a consumer-grade device tool.

The chain of custody supports both the regulatory enforcement record and the downstream litigation use of the same artifact.

“

Same forensic bench that runs MEDAL is behind COMET. The records that flow through COMET on day one are defensible to a court on day one thousand. That is the test, and it is the only test that matters.

John Wilson, Chief Information Security Officer and President of Forensics, HaystackID

Coverage Today

THE CHANNELS WHERE THE BUSINESS HAPPENS.

Across iOS and Android.

01

WhatsApp

02

iMessage

03

SMS

04

MMS

TO FOLLOW

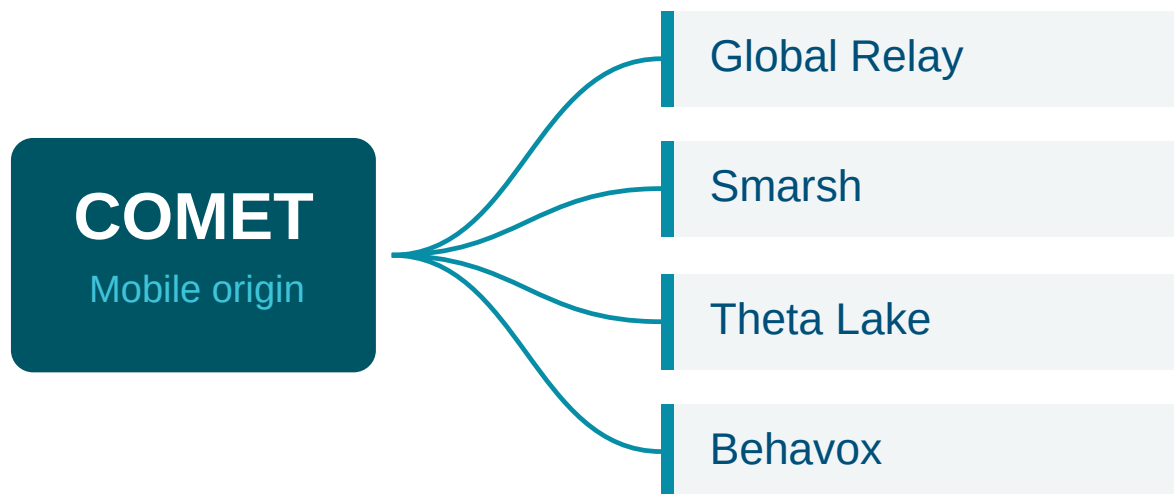
Signal and Telegram.

One defensible chain of custody, whatever the channel.

Collection, transit, archive, and access are all evidenced.

Sits With Your Archive

WE FEED YOUR ARCHIVE. WE DO NOT REPLACE IT.



COMET captures the mobile origin and retains it directly in the compliance archive you already own.

No second data store. No archive lock-in.

“

Most regulated firms have already chosen their archive. We are not asking them to choose again. We are giving them a defensible collection into the archive they have.

John Wilson, Chief Information Security Officer and President of Forensics, HaystackID

Privacy Is the Design

BUILT FOR REGULATED COLLECTION UNDER GDPR, FROM DAY ONE.



Work-Only Scope

Enforced at the custodian level.
Personal communications stay out.



Custodian Controls

Opt-in, scope, retention windows,
and termination.



Separated Residency

EU, UK, and US data-residency
paths are separated.

Built for GDPR Article 5 minimization and Article 25 privacy by design, and the EU and UK employee-monitoring regimes.

Who It Is For

BUILT FOR THE COMPLIANCE OFFICE THAT OWNS THE RECORD.

01

Chief Compliance Officer

Owns the regulator relationship
and the budget.

02

Head of Surveillance and Head of E-Comms Supervision

Own the coverage.

03

Head of Financial Crime and MLRO

Own the exposure.

The Regulatory Moment

THE OBLIGATIONS ARE ALREADY ON THE BOOKS.

LIVE SINCE 2018

MiFID II Article 16(7) and UK FCA SYSC 10A require recording of electronic communications tied to order handling.

IN FORCE SINCE JANUARY 17, 2025

DORA pulls recordkeeping into operational-resilience scope.

MARKET ABUSE REGULATION

Article 16 requires communication recordkeeping for market soundings and insider lists.

FROM AUGUST 2, 2026

EU AI Act Article 50 transparency obligations apply. COMET was built with that obligation in view.

The Article 50 applicability date is to be confirmed against the current instrument.

OPEN FLOOR

Capture it cleanly, before it becomes a fine.

COMET is available now. Start with a scoping conversation about your channels, your archive, and your exposure.

PRESENTER

John Wilson

ROLE

Chief Information Security Officer and
President of Forensics, HaystackID

EMAIL

JWilson@HaystackID.com