ACTFORE and Restoring Control After a National-Scale Healthcare Data Breach

ACTFORE

SUMMARY

In 2024, a Fortune 500 healthcare organization experienced a significant cyber incident involving the unauthorized exfiltration of sensitive healthcare, identity, and financial data. Operating at national scale, the organization supported millions of individuals across all 50 U.S. states and maintained extensive repositories of protected health information (PHI), personally identifiable information (PII), and payment data accumulated over decades of operations.

Early internal assessments produced widely varying estimates regarding the scope of the breach. While it was clear that data had been accessed and removed, uncertainty remained around the true volume of compromised material, the types of data involved, and the number of individuals potentially affected. Given the heightened regulatory obligations associated with healthcare data, leadership could not rely on directional estimates or partial visibility.

To establish a defensible understanding of the incident—and to support legally sound notification, regulatory reporting, and external communications—the organization engaged ACTFORE to conduct a comprehensive forensic data analysis under strict security and time constraints. The objective was clear: replace assumptions with verified facts and restore decision-making confidence at national scale.

RESULTS

9.6TB
of Data Analyzed

10M
primary files indexed

100M
individuals impacted

CUSTOMER DETAILS

Fortune 500 Healthcare

400,000+ Employees

Headquarters: United States

COUNSEL

Am Law 100

PROPRIETARY PRODUCTS

- BOXER
- CLARITY
- DISCOVER

THE INCIDENT & RISK LANDSCAPE

Initial assessments significantly understated the complexity of the breach. What appeared to be a large but bounded dataset was, in reality, a deeply fragmented environment spanning active systems, historical exports, backups, and nested archival structures accumulated over years of healthcare operations and compliance-driven retention.

Sensitive data was not confined to obvious repositories. Some of the most consequential records—PHI, personally identifiable information (PII), and financial identifiers—were embedded within compressed archives and legacy datasets that would not surface through conventional review methods. Without disciplined unpacking and validation, large portions of exposure would have remained invisible, introducing substantial legal and regulatory risk.

The national footprint of the organization amplified these stakes. Data tied to individuals across all 50 U.S. states was implicated, elevating the incident beyond a routine healthcare breach. Leadership faced pressure to act quickly while ensuring every conclusion could withstand scrutiny from regulators, insurers, and government stakeholders.

> The value wasn't just speed—it was confidence. Once the analysis was complete, we weren't second-guessing our decisions or worrying about what we might have missed.

Client
Chambers | Crisis & Risk Management 2025

FORENSIC RESPONSE & OUTCOMES

ACTFORE deployed a secure, on-shore processing environment to ingest and analyze the full dataset under heightened security controls. High-velocity indexing quickly established a complete analytical baseline, replacing assumptions with verified facts.

The initial scan confirmed the true scope of the breach: 9.6 terabytes of data, comprising over 10 million primary files, with tens of millions more embedded within nested and archival formats. In coordination with counsel and client leadership, ACTFORE defined 29 in-scope data elements spanning PHI, PII, and financial identifiers.

Using proprietary automation, customized extraction logic, and targeted analyst validation, ACTFORE processed nearly nine terabytes of unstructured data over a ten-week deployment. Every extracted data point was traceable to its source file, producing an audit-ready record of exposure tied to more than 100 million individuals nationwide.

By the end of the engagement, uncertainty had been replaced with a single, defensible source of truth. Notification planning became precise rather than expansive. Regulatory reporting was grounded in evidence rather than projections. Leadership, counsel, and external stakeholders were able to proceed with confidence, supported by analysis that could withstand legal and regulatory review.

REVEALING HIDDEN EXPOSURE

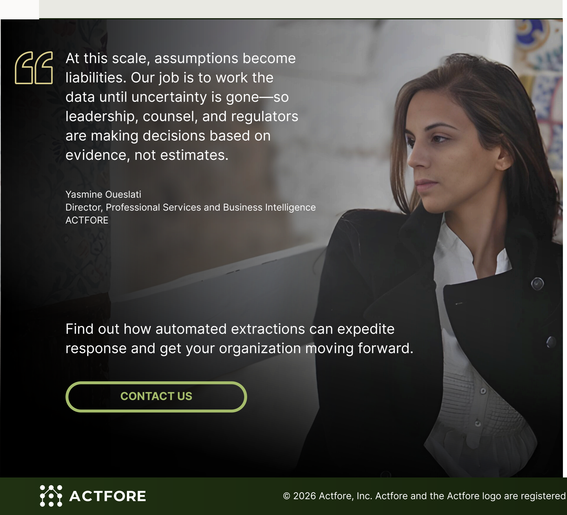
More than half of the compromised data was embedded within compressed and archival formats. Systematic unpacking was required to surface sensitive records that would have remained invisible under conventional review methods.

50M
Nested and archived files unpacked

ENABLING DEFENSIBLE NOTIFICATION DECISIONS

By defining and validating specific PHI, PII, and financial data elements, ACTFORE enabled notification and regulatory decisions grounded in confirmed exposure rather than conservative assumptions.

29
In-scope data elements



> At this scale, assumptions become liabilities. Our job is to work the data until uncertainty is gone—so leadership, counsel, and regulators are making decisions based on evidence, not estimates.

Yasmine Oueslati
Director, Professional Services and Business Intelligence
ACTFORE

Find out how automated extractions can expedite response and get your organization moving forward.

CONTACT US