Rapid Response Forensics

HaystackID Stops Internal Theft of IP at Global Healthcare Waste Company

Corporate intellectual property and trade secrets are the lifeblood of successful businesses, especially in crowded and competitive marketplaces. HaystackID understands that a rapid response is essential to identify, contain, and remediate time-sensitive threats to corporate IP.

The potential exposure, both in real dollar terms and optically within the marketplace, is significant, and the harm caused by IP loss can erase what took organizations years to develop. A recent case highlights the speed and depth with which HaystackID responded to an emergency situation to prevent the loss of critical IP due to internal theft.

Background: *A leader in innovative techniques for sharps management.* The client company is one of the largest providers of waste services in the North American healthcare sector with bio-waste management and disposal solutions across more than 20 operation sites in the U.S. along with additional sites globally.

As an industry leader, the company has developed innovative approaches to the management and disposal of sharps – objects or devices that puncture or lacerate the skin (i.e., needles, scalpels, blades, as well as certain types of glass, plastic and guidewires). Prior to these proprietary solutions, the various forms of medical, pharmaceutical, and chemotherapy waste were routinely burned in hospital incinerators.

Exposure: *Critical IP widely accessible internally.* In the healthcare waste market sector, sales cycles are long, revenue values are high, and contract terms last several years. Notably, each pending contract opportunity represents millions of dollars in potential revenues for the company. With this in mind, protecting the IP surrounding the company's sharps management techniques and practices is a high priority at all times.

The company is organized with senior business development and sales executives in regional offices throughout the United States. Each senior team member had access to contract files, pricing, R&D / Engineering reporting, financial information, and future planning in support of their pursuit of new business for the organization.

Threat: *Senior executives secretly planned to leave with company IP.* The vulnerability of company IP became an urgent issue when indications surfaced that two regional vice presidents for business development were discretely planning to leave the organization. More importantly, it appeared they were coordinating their departure while both had major contracts pending that represented a potential $10 million exposure to the company.

HaystackID Responds: *HaystackID exposes risks to identify and isolate theft.* HaystackID immediately brought in a team consisting of litigation support, consultants and forensic examiners to investigate the institutional controls that were in place and expose any possible risks.

We secured all business systems, CRM and ERP systems, network shares, and email repositories for preservation and analysis. The organization's fears were well founded based on our forensic analysis of email communication between the two individuals during the target timeframe. However, we had yet to find evidence of collusion or attempted theft of trade secrets.

We faced other obstacles. In-house counsel confirmed that neither employee's employment agreements included a restrictive covenant, leaving them free and clear to move to a competitor. Plus, the company had not fully deployed a mobile device management solution to allow examination of smartphone activity at the server.

Solution: *A preemptive sting operation captures incriminating phone data.* The company and HaystackID devised a plan to bring all regional VPs into the U.S. headquarters facility the following week under the guise of planning the rollout of new solutions for the following year. Once the attendees arrived, they were instructed to leave all phones with the company's IT department.

The HaystackID team immediately created forensic images of the phones of the two suspected executives while they were in the meeting – both unaware that their phone data was no longer secret thanks to HaystackID's extensive set of forensic tools.

Outcome: *HaystackID's fast action saved critical time and money.* The entire process took HaystackID less than a week since our initial consultation. We successfully located the damning evidence that enabled the client to immediately secure a temporary restraining order and begin pursuing further action against the two suspected internal thieves. This saved the client thousands of spend dollars and protected several million dollars' worth of projected revenue.

Learn More. Today.

Contact HaystackID today to learn more about how our highly rated eDiscovery consulting and services can enhance your ability to efficiently and economically achieve favorable investigation and litigation outcomes.

About HaystackID

HaystackID is a specialized eDiscovery services firm that helps corporations and law firms find, listen, and learn from data when they face complex, data-intensive investigations and litigation. With an earned reputation for mobilizing industry-leading computer forensics, eDiscovery, and attorney document review experts, HaystackID's Forensics First, Early Case Insight, and ReviewRight services accelerate and deliver quality outcomes at a fair and predictable price.

HaystackID serves more than 500 of the world's leading corporations and law firms from North American and European locations. Our combination of expertise and technical excellence, coupled with a culture of white glove customer service, makes us the alternative legal services provider that is big enough to matter but small enough to care. **Learn more today at HaystackID.com.**