POLARIS
CORPORATE RISK MANAGEMENT

The Polaris Approach to Internal Misconduct Investigations

In the event of internal misconduct, the long-term health of your business – and the continued trust of your clientele – depend on a timely, comprehensive assessment. When up to seventy-five (75%) percent of employees have stolen from their employers on at least one occasion, or when the average internal data breach can cost employers up to $4.9 million, your team cannot afford a slow response.

Before employee malfeasance can impact your profitability, safety, or efficiency, Polaris' consulting, investigative, and forensics teams can track and limit your exposure, helping to confirm or identify a rogue actor's intentions, methods, or access. Then, after a thorough investigative assessment, Polaris navigates clients through next steps, including termination(s), insurance recovery, or criminal prosecution.

Integrated, Proactive Services

CONSULTING MEETS DUE DILIGENCE

Your response to employee malfeasance may make the difference when managing potential fallout. Polaris consultants offer critical guidance as you chart a response, while our investigators assess employees – and their potential stressors – to limit further exposure. In an effort to uncover otherwise obscured content, investigators parlay detailed background screenings of suspected rogue actors into deeper searches and in-depth staff interviews.

PROACTIVE MONITORING & REPORTING

To promote safe, secure, and timely reporting, Polaris installs and oversees anonymous internal reporting services. Our reporting services promote a vigilant, accountable workforce, while our AI-enabled monitoring proactively identify and assess any deviations in employee activity and systems use, which may be indicative of misuse of company funds, theft, data breaches and other illicit activity.

Strategies from Certified Experts

SUBJECT MATTER EXPERTISE

Polaris' forensic accounting specialists hold a range of relevant certifications, including Certified Fraud Examiner ("CFE") and Anti-Money Laundering ("AML") certifications. These experts collaborate with investigative and computer forensics teams to assess client books, records, email correspondence, and processes, with a particular focus on identifying signs of malfeasance. These sources and methods balance hard data with human, subjective sources, including interviews with vendors and employees.

EXPERT GUIDANCE ON A PATH FORWARD

Polaris' work does not end when an individual case closes; our subject matter experts assist your team with next step efforts, including, but not limited to, preparing of a Proof of Loss report, composing documents for potential criminal/law enforcement referrals, and formulating recommendations or remediation measures.

Computer & Digital Forensics

DETAILED & THOROUGH

For investigations involving a tech-savvy employee or cyber intrusions, Polaris can conduct forensic reviews and analyses of breached servers, server logs and relevant accounts to identify notable or discernable anomalies and lateral movements. Our Technical Surveillance Countermeasure Sweeps, moreover, trace leaks to their source, identifying any bugs or other methods used by infiltrators, positioning your company for a more secure future.

In concert with our investigations team, Polaris' computer forensics team conducts meticulous screenings of technological devices and systems. Analyses may recover deleted emails, deleted computer files, data from digital bookkeeping services, previous connections to external storage drives; and more. These technical analyses will be supplemented by additional key word searches, conducted in coordination with the CFE.

CASE STUDY

When a national hospitality brand identified discrepancies in their accounts – including duplicate checks issued to its accounting manager – the Client launched an internal screening. Their discovery of further red flags prompted them to call Polaris. By analyzing employee and vendor data, our investigative team identified multiple shell companies, shared addresses, and fake personas potentially used to mask the rogue actor's payments. Meanwhile, the concurrent efforts of Polaris' forensic accounting and computer/digital forensics teams uncovered hundreds of improper payments, emails, and files – *many of which had been deleted by employees to hide their activities*. Their efforts ultimately unmasked a massive embezzlement scheme linked to a grander, apparent money-laundering operation. The Client used Polaris' proof of loss report in discussions with law enforcement, coordinated and consulted on by Polaris. The Client was soon able to recoup losses and pursue prosecution of the bad actors.