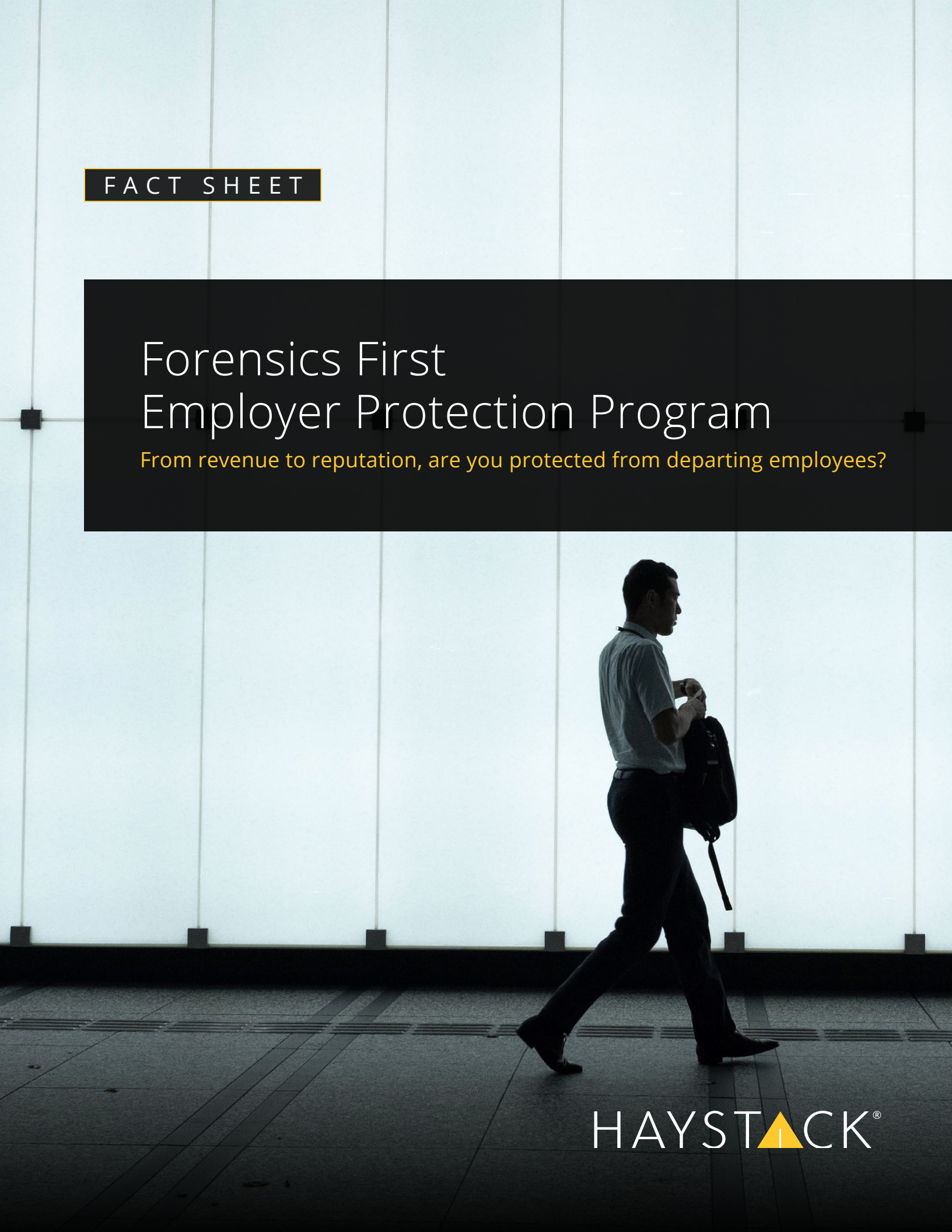
FACT SHEET

Forensics First Employer Protection Program

From revenue to reputation, are you protected from departing employees?



HAYSTACK®

Employer Protection Program

Recently one of your company's most important employees resigned to pursue other interests. The resignation was a surprise, but the reasons shared for the resignation were sound and stated as noncompetitive in nature. The exit interviews and out processing of the employee proceeded without issue. However, several months later your company experienced a surprise drop in business from those clients who previously worked with the departing employee. And after investigation and discussions with those lost accounts, you learned that upon departure the former employee had not only downloaded all key customer lists and contracts, but also the sales and product plans for the coming year. Additionally, the employee actually went to work for a direct competitor, contrary to the reason for resignation shared. This scenario is a risk nightmare experienced by many companies that do not take the proper protective measures during employee transitions. A risk nightmare that can be reduced significantly with HaystackID's Employer Protection Program.

An Overview of HaystackID's Employer Protection Program

HaystackID's Forensics First Employer Protection Program helps employers proactively reduce the risk of computer-related theft, destruction, or misuse of digital access and assets resulting from intentional or inadvertent activities associated with the voluntary or involuntary separation of employees.

Departure Risks Warranting Employer Protection

As harsh as it sounds, every departing employee poses a risk to your business if the transition is not correctly managed and documented. This risk ranges from inadvertent access to sensitive company information as basic as company internal organizational charts to deliberate efforts to acquire and use economically essential customer lists and contracts for competitive advantage. Examples of risks may include:

- Access to Regulated Data (PII)
- Competitive Analysis Compromise
- Intellectual Property Loss
- Loss of Data Subject to Legal Hold
- Proprietary Information Access
- Trade Secret Misappropriation

With HaystackID's Forensics First Employer Protection Program, our expert certified forensics examiners can help you proactively protect your organization against access, theft, and destruction of digital assets by departing employees.

Forensics First Employer Protection Program

Designed to be implemented at the time an employer becomes aware of an impending employee/employer relationship change, the Forensics First Employer Protection Program consists of passive and active protocols that deliver computer forensics expertise, audit and investigation experience, and best-of-breed technology supported by forensically sound and defensible eDiscovery best practices.

The Employer Protection Program Departing Employee Evaluation (Passive Protocol)

Consisting of a six-point evaluation that provides context for the development of a customized protection plan for departing employees, the evaluation elements include:

- Why is the employee departing?
- Where is the employee going?
- What company property must be surrendered upon departure?
- What access to company systems must be terminated upon departure?
- What potential degree of risk does management associate with the departure?
- Has the employee been advised of confidentiality, non-solicitation, and non-compete obligations?

The Employer Protection Program Departing Employee Investigation (Active Protocol)

A six-step comprehensive and customized investigation that includes but is not limited to the following forensics and collection services:

- Communication Device (Cell Phone) Imaging
- Computing Device (Laptop/Desktop) Imaging
- Device and Data Access Log Analysis
- Forensically-Sound Retention of Images
- Comprehensive Reporting of Departing Employee Investigation

The comprehensive reporting of departing employee investigation includes a package of six reports supporting the departing employee interview and investigation. Elements of the report package include:

- **Complete File Listing:** All active and deleted files from targeted devices.
- **Internet Activity:** Listing of website visits, cookies, and downloads to targeted devices.
- **Recent Document Activity:** Documents recently created, saved or downloaded to include full path and file type information.
- **System Analysis:** Key systems information including external device access.
- **Keyword Search:** File listing and all active and recoverable deleted files that contain search hits for an employer-specified number of keywords.
- **File Extraction:** An extraction of all active and recoverable deleted files of a single designated file type. Available file types include Word, Excel, PowerPoint, PDF, Standard Graphics, Video Files, Audio Files, Database Files, and Email Stores.

Delivered for a nominal flat fee based on your specific departing employee requirements, HaystackID's Employer Protection Program provides employers with timely access to key information to help employers proactively understand the state of digital data on departing employee computing and communication devices.

Learn More. Today.

Contact us today to learn more about how HaystackID can help solve your organization's departing employee challenges with our Forensics First Employer Protection Program.

About HaystackID®

HaystackID is a specialized eDiscovery services firm that helps corporations and law firms securely find, understand, and learn from data when facing complex, data-intensive investigations and litigation. HaystackID mobilizes industry-leading cyber discovery services, enterprise solutions, and legal discovery offerings to serve more than 500 of the world's leading corporations and law firms in North America and Europe. Serving nearly half of the Fortune 100, HaystackID is an alternative cyber and legal services provider that combines expertise and technical excellence with a culture of white-glove customer service. In addition to consistently being ranked by Chambers USA, the company was recently named a worldwide leader in eDiscovery services by IDC MarketScape and a representative vendor in the 2021 Gartner Market Guide for E-Discovery Solutions. Further, HaystackID has achieved SOC 2 Type II attestation in the five trust service areas of security, availability, processing integrity, confidentiality, and privacy. For more information about its suite of services, including programs and solutions for unique legal enterprise needs, go to HaystackID.com.