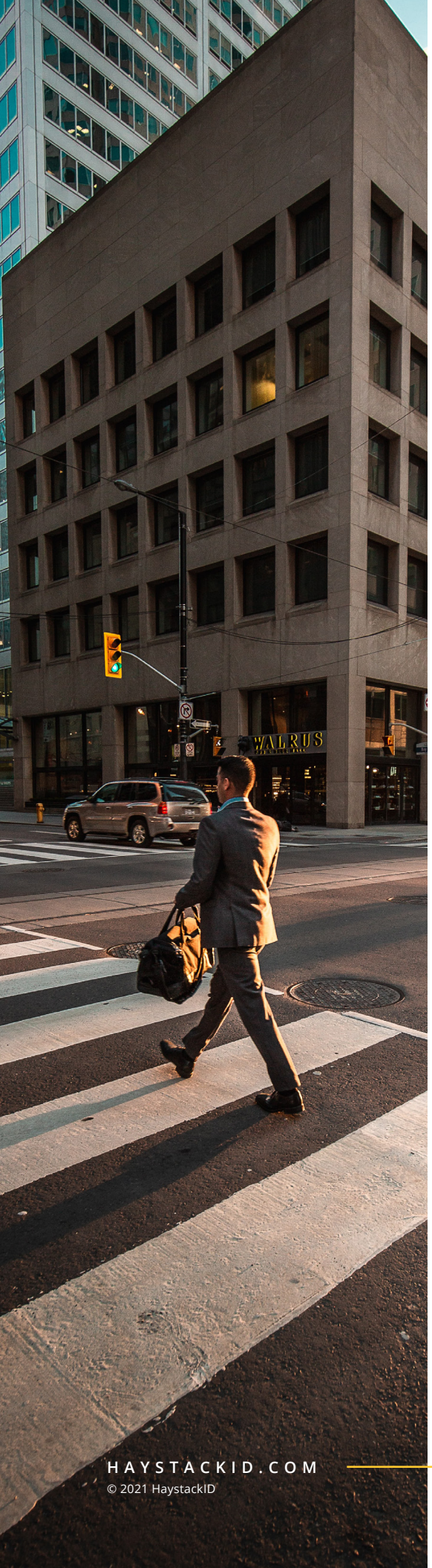
INFORMATION SHEET

Departing Employees? Employer Protection Program Options

Understanding Program Options and Details

HAYSTACK®



Summary

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 unintentional activities associated with an employee's voluntary or involuntary separation.

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.

Proactive Protection From Departed Employees

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.

To help employers manage and mitigate potential departing employee risk, HaystackID provides proactive protection from departed employees through its Employer Protection Program. With this program, HaystackID's expert certified forensics examiners can help you proactively protect your organization against access, theft, and destruction of digital assets by departing employees. This proven program provides you with a range of offerings that span the spectrum from premium protection and full reporting to targeted protection with selected reports. Corporations and organizations can purchase Employer Protection Program support, choosing from three options designed to balance required protection and ease of business engagement.

Three Options to Mitigating Departing Employee Risk

HaystackID's forensics team will conduct option-based preservation and analysis work and provide reporting as appropriate to demonstrate our findings.

Option One: Premium Protection (Full Menu Support per Custodian)
Option Two: Proven Protection (Targeted Menu Support per Custodian)
Option Three: Defined Protection (Customer Defined Support)

Pricing Model	One	Two	Three
Flat Fee per Custodian	X*	X**	
Per Hour Support			X

** (1) Laptop/Desktop, (1) Mobile Device, and (1) Email Account.*
***(1) Laptop/Desktop OR (1) Mobile Device) and (1) Email Account*

Other Services	One	Two	Three
Data Remediation*	X	X	X
Forensic Analysis (Burst Outside of Flat Fee)*	X	X	X
Expert Testimony/Affidavit and Declaration Creation*	X	X	X
Data Preservation/Collection			X

** Outside of Flat Fee if applicable.*

Evidence Preservation	One	Two	Three
Creation of a forensic mirror image of the computer asset(s), including a redundant backup copy to guard against media failure, and generation of all necessary documentation (chain of custody and preservation details).	X	X	

Computer Basics	One	Two	Three
Operating system present/date of installation/time zone settings for the computer.	X	X	
User profiles present on the drive and dates of their creation.	X	X	
Partition information for the computer's hard drive(s) (e.g., numbers, sizes, types), and whether logical partitions account for the drive's full physical size (which, if not, can be suggestive of hidden partitions/data).	X		
Any indicators of the computer not being used or being rolled back to a base image prior to acquisition.	X		
List of user profiles present on the computer, along with their dates of first/last login (where available).	X		

Data Exfiltration Evidence	One	Two	Three
External device connection history (index of USB storage devices connected to the computer, along with their dates of first connection and, where possible, dates of recent activity).	X		
Indicators of data exfiltration (e.g., Windows link file analysis, recent creation of compressed container files, access to cloud storage sites such as Dropbox. For Mac systems, this would include examination of relevant .plist files that contain evidence about recent activity).	X		
HaystackID recommends that an audit log of the departing employee's recent Salesforce/CRM activity be provided and compared to the internet history found on the work computer. Obvious discrepancies between the two could suggest that a personal computer device was used for exfiltration.	X		
Look for evidence of device backups and examine/ process accordingly.	X		
Inventory of files and file types contained on the drive, in the form of First Contact reporting.		X	
List of external devices connected, as evidenced by the Windows registry and log files, indicating make/model/serial number and available dates of connection.		X	
List of applications found installed on the computer.		X	

Deletion/Wiping Evidence	One	Two	Three
Overview of Recycle Bin/Trash/Bin artifacts.	X		
Indications of wiping activity (e.g., installed applications, references to applications being run, strange MFT artifacts often created by wiping tools).	X		
Summary assessment of deleted user-type files on the computer (e.g., an absence of any deleted files can suggest prior use of a wiping tool, and a broad range of recoverable deleted files can suggest against that conclusion).	X		
Status of data in the drive's unallocated clusters (a.k.a. free/empty space) – a typical indicator of wiping is free space being completely blank or filled with repetitive data patterns.	X		
Summary listing of deleted folders and files, as evidenced by: (a) Recycle Bin/Trash/Bin artifacts; (b) deleted MFT records still visible in the active file system (this will be contained in the second tab file listing of the First Contact reporting).		X	
"First look" only/preliminary analysis re: evidence of data wiping/ scrubbing/permanent deletion utilities, via such utilities being found currently installed and/or run (via a registry artifact called UserAssist).		X	

Recovery/Parsing of "Private" Communications	One	Two	Three
Survey of installed instant messaging/chat applications (Skype, Yahoo! Messenger, etc.)	X		
Attempt to programmatically recover IM/chat content artifacts.	X		
Attempt to programmatically recover artifacts of webmail use (Gmail, Yahoo!, etc.)	X		
Evaluate with customer the appropriateness of conducting second-level recovery/analysis of these communications (e.g., can sometimes recover additional content fragments using more manual/tedious methods).	X		

Focused Keyword Searches of Forensic Drive Images	One	Two	Three
Run searches against the forensic image for 20 or less narrowly tailored and well-crafted keywords (e.g., names of competitors, known email addresses, etc.) Depending on the volume and nature of hits encountered, our deliverable may be either or both: the hit files themselves (if they can be reviewed easily by the customer); or summaries of the hits with "previews" of the hits' context.	X		

NOTE: *Searching for generic terms or acronyms against forensic drive images commonly produces unmanageable volumes of hits, e.g., in the millions. HaystackID will consult with the customer to help tailor these searches appropriately and to prioritize the review of hits that are encountered. Where voluminous hits are nonetheless encountered, we will consult with the customer to prioritize what hits are reviewed and in what order.*

Focused Keyword Searches of Locally Stored Email Content on the Computer	One	Two	Three
Attempt to recover so-called "unpurged" or "double-deleted" email items from within the email storage files on the hard drive being examined (many email software client applications retain items that have been emptied from the deleted items bin, and these can sometimes be recovered using forensic tools).	X		
Index and search both the active and recovered, double-deleted email items for narrowly tailored keywords. summaries of the hits with "previews" of the hits' context.	X		

Internet Browser History/Artifacts	One	Two	Three
Indication of which internet browsers are installed, and which appear to contain substantive artifacts.	X		
Programmatic compilation of internet browsing history on the computer, resulting in a searchable index that the customer can review. HaystackID will also attempt to highlight for the customer any behavior deemed potentially relevant.	X		

NOTE: *Detailed, hands-on review of this data by HaystackID can become very time-consuming, and in some cases may trigger the need for supplemental budget. Again, HaystackID will apprise the customer of this and provide budget estimates on a case-by-case basis.*

Comprehensive Reporting	One	Two	Three
Comprehensive report provided of our findings.		X	
Complete File Listing: Key Findings Report. All active and deleted files from targeted devices.	X	X	
Internet Activity: Listing of website visits, cookies, and downloads to targeted devices.	X		
Recent Document Activity: Documents recently created, saved, or downloaded to include full path and file type information.	X		
System Analysis: Key systems information including external device access.	X		
Keyword Search: File listing and all active and recoverable deleted files that contain search hits for an employer-specified number of keywords.	X		
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, and Standard.	X		
Graphics, Video Files, Audio Files, Database Files, and Email Stores.	X		

Learn More. Today.

Contact us today to learn more about how HaystackID's expert team and proven technology can help solve your organization's departing employee challenges with our 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.