Identifying PII while Maintaining Client Data Integrity & Security

Digital Forensics & Managed Review – Case Study

Innovative Discovery, LLC

Context

The Client, a prominent distributor in the food & beverage industry, requested assistance from Innovative Discovery, LLC ("ID") with an internal investigation of a terminated employee's laptop. The laptop contained Personally Identifiable Information ("PII") from their customer base, which raised the Client's concerns about privacy protection. In order to provide a full disclosure to the court, the Client needed to analyze the information the laptop contained and identify the extent of the PII that was potentially released.

Challenges

- No access to original employee laptop, therefore Client provided ID an encrypted backup copy on a hard drive.
- Client did not know the full extent of PII that was contained on the laptop
- Court-mandated deadline to provide comprehensive report of PII.

What is Personally Identifiable Information ("PII")?

The Office of Management and Budget (OMB) defines personally identifiable information as:

"information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc."

Common Examples of PII:

- Social Security Number (SSN)
- Passport Number
- Patient Identification Number
- Credit Card Number
- Driver's License Number
- Internet Protocol Address or other Asset Information

Collection Process

Using the encrypted backup copy of the laptop provided, the Client's initial instructions were to search for PII based on customer social security numbers. ID's Digital Forensics team assessed the data and suggested expanding the investigation to include pattern searches of social security numbers, bank routing numbers, and credit card numbers. Within 48 hours of receiving the backup copy, imaging and pattern searching was completed and all data responsive to the pattern searches was then loaded into a Relativity workspace for review.

Managed Review

Once the data was transitioned to the Managed Review team through the Relativity workspace, ID assembled a team of reviewers with experience specific to identifying various types of PII. As the review team moved through the documents in the workspace, each reviewer identified the customer name, type of PII, and any contact information available. Each reviewer's coding decisions were subject to a thorough Quality Control process and the final results were exported into a comprehensive report for the client. The Managed Review portion was completed in approximately ten days and the entire process, from receipt of laptop data to delivery of final PII report, was completed in less than two weeks.

	A	B	C	D	E	F	G	H	I	J	K	L
1	Identifier	Single Instance / Has Duplicate(s) / Is Duplicate	MD5 Hash	PII - PII Type I	C11 - PII - Address1	C11 - PII - EmailType	C11 - PII - First1	C11 - PII - Last1	C11 - PII - Middle1	C11 - PII - Phone1	C11 - PII - PhoneType	C11 - PII - SSN1
2	ABCD-PII-0000415	Has Duplicate(s)	D76B9814CB0A601A0B0F1AC4D014EE66	SSN	1700 N. Moore St Apt. 1500 Centreville, VA 20120	N/A	Quincy	Earl	Jones	(Home) 555-555-5555; (Alternate) 555-555-5555	Unsure	111-11-1111
3	ABCD-PII-0001111	Is Duplicate	D76B9814CB0A601A0B0F1AC4D014EE66	SSN	1700 N. Moore St Apt. 1500 Centreville, VA 20120	N/A	Quincy	Earl	Jones	(Home) 555-555-5555; (Alternate) 555-555-5555	Unsure	111-11-1111
4	ABCD-PII-0001618	Single Instance	5C6D07115E4F2830151794DB988B964D	SSN	9669 Miracle Salad Ave Suite 82 New York, NY 10001	N/A	Jones	Latham	Jeremiah	Not Available	N/A	111-11-1111

Due to the highly sensitive nature of the investigation, one of the Client's main concerns was the secure transferal of data throughout the collection and review process. ***ID's ability to provide end-to-end services in-house significantly reduced the risk of exposure when compared to the risk associated with transferring the data from a Forensics service provider to a Managed Review service provider.*** By working closely with ID's Digital Forensics department to determine patterns in PII information and the Managed Review department to compose an extensive final report, the Client was able to meet their court-mandated deadline, avoid data breach liability and further exposure to the company and their customers.