# IDENTIFYING PII WHILE MAINTAINING SECURITY

## A DIGITAL FORENSICS & MANAGED REVIEW CASE STUDY

### THE SITUATION

The client, a prominent distributor in the food & beverage industry, needed help with an internal investigation of a terminated employee's laptop that contained personally identifiable information (PII). In order to provide a full disclosure to the court, the client needed to analyze the laptop and identify the extent of the PII that was potentially released. Because there was no access to original laptop, the client provided ID an encrypted backup copy on a hard drive.

### THE SOLUTION

Using the backup copy, ID's digital forensics team assessed the data and expanded the investigation to include pattern searches of social security numbers, bank routing numbers, and credit card numbers. Within 48 hours of receiving the backup, imaging and pattern searching was completed and all data responsive to the searches was loaded into a Relativity workspace for review.

Once the data was transitioned to the managed review team, ID assembled a team of reviewers with experience specific to identifying various types of PII. The review team identified the customer name, type of PII, and contact information. 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 RESULT

The managed review was completed in ten days and the entire process, from receipt of laptop data to delivery of final PII report, was completed in under two weeks. ID's ability to provide end-to-end services in-house significantly reduced the risk of exposure. The client met their court-mandated deadline, avoiding data breach liability and further exposure to the company and their customers.