B6 Preventing a Rush to Judgment: Application of Computer Forensics in Data Breach Cases

Jason M. Paroff, JD, Kroll Ontrack, 1 Harmon Meadow Boulevard, Suite 225, Secaucus, NJ 07094; Stephen D. Baird, MS, Kroll Ontrack, 1166 Avenue of the Americas, 23rd Floor, New York, NY 10036; and Alan E. Brill*, MBA, Kroll Ontrack, 1 Harmon Meadow Boulevard, Suite 225, Secaucus, NJ 07094*

After attending this presentation, attendees will understand how the pressures on corporate and governmental managers who believe that their organization has been the target of a successful breach of sensitive personal or health-care data can lead to jumping to conclusions that, in fact, a suspected breach is a real one. This can result in the notification of thousands of people, informing them that they have been victims of an incident that, in fact, never occurred. The application of computer forensics often provides the best way of determining whether an actual

incident occurred and whether that incident meets the varied criteria for victim notification under the 47 United States State laws, plus applicable United States and international federal laws and regulations.

This presentation will impact the forensic science community by demonstrating that through the use of digital forensics, companies can avoid needless large outlays for notification and remediation cost if it can be shown with forensic accuracy that an incident did not occur (or that it is different in scope than assumed) and avoid the creation of unnecessary anxiety on the part of persons who would be concerned about identity theft when, in fact, their data was not at risk.

When an organization has reason to believe it has suffered a breach of sensitive personal or health-care information, there are literally dozens of state and federal laws and regulations that may, depending on the nature of the data compromised, and the home jurisdiction of the individuals involved, require specific notification of affected individuals as well as governmental entities. These notifications are often tied to tight timelines in the law, but it has been found that with proper project control and forensic discipline, an investigation can be carried out within the allotted time frames that can provide management (and usually counsel) with the best information available to support their decision making process. Recent surveys indicate that the cost to an organization of a data breach can exceed $20 per victim simply for notification and basic remediation assistance, so breaches of as little as 50,000 records can quickly result in a million dollar unplanned expense. This is, of course, in addition to what can be substantial costs related to reputational damage, and the potential costs of litigation, or added regulatory oversight that can result from reported cases of data loss – even where it is later found that the event did not actually occur.

The forensic work has the added benefit, in many cases, of providing valuable insights into exactly what happened, the vector through which an incident originated, and sometimes information about the perpetrators. It is not unusual to be able to provide some assurance that an incident has been stopped and that there is not a continuing leakage of sensitive data.

A series of case studies based on the team's work that will demonstrate actual situations in which computer forensics proved that an incident did not occur, or that it was less severe than had been assumed will be provided.

Data Breach, Personal Data, Data Compromise

 ** Presenting Author*