

## Global Data Privacy and Security Team

# Retaining A Forensic Investigator: Data Breaches At A Glance

Many competent IT departments lack the expertise, hardware, or software to preserve evidence in a forensically sound manner and to thoroughly investigate a security incident. In-house counsel needs to be able to recognize such a deficiency quickly -- and before evidence is lost or inadvertently destroyed -- and retain external resources to help collect and preserve electronic evidence and investigate the incident.

Although in the midst of an emergency you may feel that you have relatively little leverage to negotiate preferable terms in a service agreement, given the sensitivity of the information to which the investigator will have access it is essential to make sure that your service agreement contains the most protective provisions possible.



**\$0 - \$1.5 million**

Range of forensic investigation costs\*

Bryan Cave's Global Data Privacy and Security Team has responded to hundreds of data security breaches and routinely helps clients, before a breach happens, analyze and improve upon their ability to respond to a breach if (or when) one occurs.

For more Information Contact:

### David A. Zetony

Partner

david.zetony@bryancave.com

1155 F Street, N.W.

Washington, D.C. 20004

phone: 202 508 6000

### Jena M. Valdetero

Partner

jena.valdetero@bryancave.com

161 North Clark Street, Suite 4300

Chicago, IL 60601-3315

phone: 312 602 5000

### What to consider when retaining a forensic investigator:

- ✓ Does the forensic investigator have sufficient expertise to conduct the investigation?
- ✓ Does the forensic investigator have sufficient capacity to immediately deploy resources to timely investigate the incident?
- ✓ Is there a master service agreement in place?
- ✓ Does the agreement contain data security provisions that are appropriate for a contractor that is likely to gain access to sensitive personal information?
- ✓ Does the agreement contain data privacy provisions that are appropriate for a contractor that is likely to gain access to sensitive personal information?
- ✓ Is the agreement structured to protect privilege?
- ✓ Does the forensic investigator understand what is expected of them to maintain privilege protections?
- ✓ Does the service agreement include sufficient protections in the event that the forensic investigator is itself breached?
- ✓ If the organization has cyber-insurance, is the forensic investigator a preferred provider and/or approved by the insurer?
- ✓ Does the forensic investigator represent a business partner that may have an interest in the incident? If so, is there a potential conflict of interest?

\* Statistics based upon cyber liability insurance claims. NetDiligence Cyber Claims Study at 12 (2014)