Koller’s practice as a member of Baker & Hostetler's privacy and data protection group is focused on data breach response and security compliance. His background in information technology has led to his qualifications as a certified information systems security professional, a certified computer forensic examiner and as a fellow of information privacy from the International Association of Privacy Professionals.

“I go back a way with this,” he said. “Organizations are increasingly under attack. Perps and attackers recognize the value of information and the profits to be had. Over the past year I have helped clients with more than 400 different breach investigations, spanning the health care, hospitality, retail, education and technology industries and involving ransomware, phishing incidents, stolen devices and nation-state sponsored attacks.”

He advises clients in the financial, health care and retail sectors; he represents clients in Financial Industry Regulatory Authority and state attorneys general investigations and enforcement actions for alleged data security and privacy violations.

“At the same time that more attacks are occurring, there are increasing numbers of laws and regulations. The first data breach statute in California came in 2003, and subsequently almost every state has followed. And the statutes vary: Who has to be notified? Is there a risk-of-harm threshold? Even if you are a small California corporation, you may be subject to the statutes of the state where the target resides.”

Los Angeles officials called Koller when the county’s social services hotline inadvertently exposed personal data stored online in a cloud repository maintained by 211 L.A. County, the nonprofit that operates the county’s 211 hotline linking callers to community information and referral services. The data includes sensitive information about calls regarding mental health and abuse. The breach was exposed in April 2018. Also that month Koller was retained by Long Beach Community College when computers there were breached in a malware attack. In January 2017, Palomar College in San Marcos called Koller after learning that more than 3,000 people who worked at the school might have had their W-2 tax documents exposed.

“My role is that of the firefighter when you first discover the fire,” he said. “Who was impacted? What happened? The sheer volume is enormous. Last month on the Friday before Christmas week five or six matters came in.” Koller said the deluge—not all were reportable breaches—wasn’t entirely unexpected, because bad actors often time their system intrusions to occur late on Fridays and just before major holidays when they hope vigilance is low.

“We stand by to field phone calls, bring on forensic vendors, make plane reservations to get response experts to the client site asap,” he said. “The client needs quick response times, and we supply them.”