BakerHostetler's award-winning **Digital Assets and Data Management (DADM) Practice Group**, selected for Vault's "Guide to Legal Practice Areas" for the seventh consecutive year, serves Fortune 500 clients as well as health systems, universities, global retailers, small and midsize businesses, and state and municipal entities. Our seven integrated teams address risks, disputes, compliance and opportunities throughout the life cycle of data, technology, advertising and innovation, including brand strategies and monetization. Our annual "Data Security Incident Response Report" is an industry-leading resource for cybersecurity trends, breach response and best practices for data protection.

A highly respected trailblazer in the field of data security and privacy, **Ted Kobus** leads the DADM Practice Group of more than 100 attorneys and technologists nationwide. Representative clients include Marriott, Duke University, Sephora and Mayo Clinic. Under his leadership, the DADM Practice Group has earned recognition from industry heavyweights such as BTI, *Law360*, ALM and Vault. Ted also provides pertinent insights when contacted by major media outlets looking for comments on the latest news and trends in privacy and data security.

For more information, visit www.bakerlaw.com/DigitalAssetsDataManagement.

BakerHostetler

bakerlaw.com

BakerHostetler

Elise Elam, Associate, and Sara Goldstein, Partner—Digital Assets & Data Management

Elise Elam guides clients through data security matters, including coordinating digital forensic investigations, determining breach notification obligations, overseeing the implementation of restoration efforts, and responding to regulatory inquiries. As a Certified Information Privacy Professional with a master's degree in information technology, Elise bridges the gap between legal, business, and technology perspectives for clients.

Named a 2021 "Rising Star" by *Law360* and a 2021 "Lawyer on the Fast Track" by *The Pennsylvania Legal Intelligencer*, Sara Goldstein has advised hundreds of clients from a variety of different industries on responding to cybersecurity and data privacy incidents, including several of the largest data breaches to date. Sara has led BakerHostetler's response to several large, high-profile data security incidents, including one incident at a cloud software company that involved the data of several hundred firm clients. As the leader of these matters, Sara developed the strategy for the incident response process, oversaw the team of attorneys working directly with clients, and created processes and protocols for the attorney team to follow.

Describe your practice area and what it entails.

We practice cybersecurity incident response, which means we help our clients prepare for and respond to data security and privacy incidents. This includes engaging cybersecurity investigators and other third parties to assist with the incident response process; providing guidance on federal, state, and international breach notification law requirements, as well as contractual notification obligations; drafting notification materials, including notification letters, press releases, website notices, internal client communications, and regulatory notices; and representing clients in post-incident regulatory investigations.

What types of clients do you represent?

Sara represents clients in a variety of sectors, including healthcare, energy, and higher education.

Elise represents pretty much every other type of client, with a focus on clients in the insurance industry.

Both of us represent large and small companies, nonprofits, financial institutions, government agencies—you name it.

What types of cases/deals do you work on?

We represent clients responding to all types of data security and privacy incidents, ranging from business email compromises to inadvertent disclosures to ransomware and state-sponsored, large-scale network intrusions.

How did you choose this practice area?

Sara: My interest in data privacy and security began during my law school co-op internship in the office of general counsel at a large research university. I was asked to prepare research memoranda on the Genetic Information Nondiscrimination Act of 2008, which had recently gone into effect, and on new state breach notification laws, and became interested in the then-emerging area of the law.

Elise: Very deliberately. Prior to practicing incident response, I found myself searching for something that would provide more of a challenge. It was a natural fit given my interest in technology.

What is a typical day like and/or what are some common tasks you perform?

There is no typical day in incident response, and everything we work on is a crisis! No day is ever the same, and it never turns out exactly the way you planned. A typical day consists of numerous conference calls with clients, forensic investigation firms, public relations firms, and other partners in the incident response process. We also draft numerous commu-

nications ranging from reactive media holding statements to breach notification letters to legal memoranda.

What training, classes, experience, or skills development would you recommend to someone who wishes to enter your practice area?

A great way to learn more about incident response is to listen to podcasts and read blogs prepared by cybersecurity experts.

What is the most challenging aspect of practicing in this area?

The combination of the volume plus the fast-paced and—usually—urgent nature of this practice area can make it challenging to keep up and stay on track. But we enjoy helping clients navigate through some of the most challenging days of their professional careers and getting them to "the other side" of an incident. A common misconception is that incident response counsel's only (or primary) purpose is to protect privilege. In truth, we advise our clients on their legal obligations with respect to investigating cybersecurity incidents, determining what data is at risk, and their notification requirements to individuals and regulators.

What are some typical tasks that a junior lawyer would perform in this practice area?

Typical tasks that a junior lawyer would perform in this practice area include:

- Responding to different types of cybersecurity and data privacy incidents, including business email compromises, device theft/loss, system misconfiguration, ransomware, insider wrongdoing, and vendor breaches.
- Participating in initial calls with clients and forensic scoping calls.
- Reviewing and revising engagement agreements for third parties being retained to assist with the incident response process.
- Drafting communications to clients and other stakeholders involved in the incident response process.
- Answering questions from clients and others involved in responding to incidents.
- Taking detailed notes on all conference calls.
- Reviewing and assessing findings from forensic investigations to determine whether an incident results in unauthorized access to or exfiltration of data that could trigger notification obligations.
- Working with forensic investigators on drafting/editing forensic investigation reports and factual summaries.
- Researching federal, state, and international breach notification law requirements.
- Drafting notification materials, including notification letters, press releases, website notices, internal client/employee communications, third-party stakeholder notices, and regulatory notices.

What are some typical career paths for lawyers in this practice area?

There are many different career paths for attorneys in incident response. While some associates stay with their law firms and advance to partner, other lawyers opt to go in-house at companies to support their cybersecurity and data privacy practices, and still others opt to join forensic investigation or PR/crisis management firms. There are many possibilities out there!

Given how quickly technology is evolving, how do you stay ahead of the curve and prepare for issues that may arise?

We listen to podcasts and read articles and blog posts. We also have a very collaborative team of colleagues, and we constantly share new intel on emerging trends. Also, the cybersecurity forensic investigation firms we partner with provide us with periodic education on the cybersecurity landscape they are encountering.

BAKERHOSTETLER

> "The combination of the volume plus the fast-paced and—usually—urgent nature of this practice area can make it challenging to keep up and stay on track. But we enjoy helping clients navigate through some of the most challenging days of their professional careers and getting them to 'the other side' of an incident."
>
> ***Elise Elam, Associate & Sara Goldstein, Partner***