Insult to Injury: Is the theft of your trade secrets also a data breach that requires notice?

Zach Willenbrink
414.287.9463
zwillenbrink@gklaw.com

Ashley Madsen
414.287.9495
amadsen@gklaw.com

The information contained herein is based on a summary of legal principles. It is not to be construed as legal advice and does not create an attorney-client relationship. Individuals should consult with legal counsel before taking any action based on these principles to ensure their applicability in a given situation.

The loss of trade secrets can have crippling effects on a company's business. So, it's understandable why, in the aftermath of learning about a theft, you might not automatically think, "Was this a data breach? And do we need to notify people?" You've suffered injury from the theft… do you really need to broadcast that you suffered a data breach and suffer insult, too?

Unfortunately, the answer may be "yes." You *might* have to send out those notices. But the notice process certainly beats liability for violating state statutes, regulatory enforcement, and civil lawsuits by clients—all of which (*and more*) can result from a failure to provide adequate notice.

This article highlights some of the key considerations for determining whether you've suffered a breach and, if so, for determining your notification obligations. It also provides a few suggestions on steps you can take *now* to reduce the likelihood that a trade-secret theft will also trigger notification obligations.

Is it a breach?

The definition of a breach varies from state to state, from regulator to regulator, and from contract to contract. But, generally, when deciding whether there has been a "breach," you should look for: ***unauthorized access to personal information***.

However, even with that simplified definition, it can be remarkably difficult to determine whether a cybersecurity event—like theft of trade secrets from your business' servers—is, for legal reasons, a breach that requires notification.

Determining unauthorized access, for example, can require both a tech-heavy forensic analysis and a detailed legal one. You'll probably need a forensic analysis to determine whether there was access—to your system as a whole and, at a more granular level, to personal information. And access can come in any number of flavors, from having your system hacked by a sophisticated attacker carrying out "corporate espionage" to a former employee using credentials your business forgot to cancel to log into your systems. Whether or not this access *happened* typically requires a forensic investigation by someone with technical skill. And, if they determine, yes, there was access, the next question is whether the access was authorized. This can be just as tricky. The Supreme Court's 2021 *Van Buren* decision held that an employee's use of valid credentials for an improper purpose did not violate the Computer Fraud and Abuse Act of 1986. *Van Buren v. United States*, 141 S. Ct. 1648 (2021). Since then, lower courts have struggled to define what *exactly* makes access unauthorized; and how (or whether) this impacts breach reporting remains to be seen.

If you determine there was unauthorized access, you'll need to figure out exactly *what* was accessed. Did the trade-secret thief poke through your entire database—including, for instance, your personnel, customer, or end user files—looking for the trade secrets they were really after? If so, they might

have accessed personal information along the way… *even* if that access was unintentional, *even* if that access was brief, and *even* if the intruder didn't copy or remove a single piece of personal information.

At bottom, the breach determination is context-specific, changing depending on the facts and on the law. It's a determination best made with the help of both a knowledgeable attorney and a forensic investigator.

What are your notification obligations?

Let's assume you decide there was a breach. Who do you have to notify? When? What do your notices have to include?

Start with the group most people think about when in the context of "breach notifications": individuals whose personal information was affected. Many state statutes require notice to these individuals as soon as practicable or within a specified time frame (often 30 days), and that the notices contain different details about the breach.

Statutes or regulations may also require you to notify state attorneys general, other law enforcement bodies, your regulators, and/or all major credit reporting agencies. Again, this obligation will vary state by state and is typically completed alongside the individual-notification process.

Unfortunately, you need to consider more than just statutes and regulations: any of your business' third-party contracts may have reporting obligations, too. And, depending on how those provisions are phrased, they may even have a lower threshold for reporting than statutes and regulations.

In making all these determinations, experienced breach counsel will generally know what is required by each state or governing entity, as well as the most efficient way to send out notices.

How can you limit the likelihood a theft becomes a breach that requires notification?

If you want to reduce the possibility that a theft turns into a breach, there are several things you can do *right now* (or, let's be honest, probably with the help of your IT team):

1. **Minimize your data** by developing a retention policy that also specifies when unused data will be deleted. The less data you have, the less likely any piece of it will be breached.

2. **Segregate your data.** Don't keep your trade secrets in the same place in your database where you also keep your personnel, customer, or end-user data files. This limits the likelihood that someone hunting for your trade secrets will accidentally stumble into the personal information you keep.

3. **Encrypt your data** (or at least your most sensitive data) even when it's at rest on your servers. Generally, even if someone accesses your data, notification obligations won't arise if the data is unintelligible to that person.

4. **Create, follow, and enforce policies that reduce the likelihood of unauthorized access.** This can include adopting understandable acceptable use policies, implementing least-privilege access that restricts your most sensitive information to need-to-know users, and carrying out procedures for immediately removing access and deleting accounts for all departing employees.

* * *

If, despite your best efforts, you suspect trade secret theft has occurred at your company, don't forget to perform this important analysis. Quick action and a thorough investigation are necessary to keep the insult of notification obligations from becoming yet another—perhaps even bigger—injury. For more information on data breaches, or to learn how Godfrey & Kahn can help, please contact Zach Willenbrink, Ashley Madsen or a member of our Data Privacy & Cybersecurity or Non-Compete & Trade Secrets practice groups.