Does Getting a Breach Notice Mean Bad Guys Have My Data?

Is it Time to Freak Out or Not?

Understanding the difference between a disclosed breach and a circulating breach can change how you respond. And whether you actually need to panic.

Every few months, another “we take your privacy seriously” email lands in your inbox. Most people shrug. But not every breach notice means your data is floating around. And knowing the difference matters.

Let’s unpack what’s really going on.

Evolution of a breach			
Breach →	**Disclosed** →	**Circulating** →	Exploited
Every day	*About 60,000*	*About 1,000*	*Unknown*

Two Very Different Kinds of Breaches

When you hear about a breach, it can fall into one of two categories: **Disclosed** or **Circulating.** Knowing which kind you’re dealing with makes all the difference.

>> Disclosed Breaches :: Public, but Not Yet Circulating

A **Disclosed Breach** is one that’s been reported or confirmed publicly. The company might have filed with the SEC, told the press, or notified customers. The key detail: **the stolen data hasn’t been observed circulating on open or dark web sources.** That doesn’t mean it’s safely contained. Only that it hasn’t surfaced publicly.

> Sidebar: Your stolen data may not be in active circulation. It may never appear publicly.
>
> But it could still be in play privately. In criminal exchanges, nation-state archives, or exclusive data markets. Treat “not circulating” as unknown risk, not no risk.

What this means:

- The data may still be in the hands of the attacker or the company's investigators.
- There's no evidence it's being sold, traded, or indexed.
- The breach appears in official reports but isn't searchable or downloadable by third parties.
- If you are being notified of a Disclosed Breach this is likely because the company is legally required to notify you that they realize your data has been compromised in some way. They may not even know where it is. (Regulations often require notification even when there's no evidence of data misuse.)

Scale:

- Over **60,000 disclosed breaches** exist globally.
- Around **5,000–10,000 new disclosures** happen every year.

So: Getting a notice from a disclosed breach doesn't mean your data is safe. It means the breach has been acknowledged. But not yet confirmed as circulating. Disclosed breaches can still transition into circulation later.

>> Circulating Breaches :: When the Data Is Out There

A Circulating Breach is when the stolen data actually hits the wild. It's uploaded, sold, or shared on criminal forums, and often becomes part of searchable services like Have I Been Pwned or DataBreach.com. Lots other entities scoop that up too, like intelligence tools, data brokers, and foreign governments.

Because that's when things shift from theoretical to real.

What this means:

- Your data is actively circulating online.
- It can be found, reused, or sold multiple times.
- It's indexed by breach search engines and often resold by automated bots.
- If you are being notified of a Circulating Breach this is likely because the you signed up for an alert service like ObscureIQ. Notification from us means that your data has come into play.
- It's possible that data from breaches that have happened years ago can hit the dark web as a fresh release. This can still be dangerous, so don't ignore such alerts out of hand.

Scale:

- Roughly 1,000–1,200 known circulating breaches exist.
- They contain billions of searchable records.

Example: The 2012 LinkedIn breach was disclosed early—but didn't circulate widely until 2016. That's when the stolen data became searchable and weaponized.

That's why ObscureIQ monitors multiple breach intelligence sources.
To alert our clients the moment their data moves from disclosed to circulating.

So, Should You Freak Out?

Not necessarily. But you should **understand where your risk really sits.**

- A **Disclosed Breach** = low immediate risk, but stay alert.
- A **Circulating Breach** = act now. Change passwords. Freeze credit. Increase vigilance.

However, if the stolen data includes sensitive credentials (such as crypto wallet keys, account passwords, or MFA data) you should act immediately, even if that breach isn't known to be circulating.

The real problem is when a disclosed breach transitions to circulating. That's when the threat becomes active.

Why "Not Circulating Yet" Doesn't Mean Safe

Sometimes, data from a disclosed breach never surfaces publicly. But it's still being used.

- **Nation-state actors** may keep stolen data private for years.
- **Criminals** sometimes sell exclusive access to a single buyer.
- That data may resurface later, as leaks tend to get resold, copied, and shared.

So, while a disclosed breach might not be "circulating," it can still carry hidden risk.

How to Think About Breach Notices Differently

Next time you get a breach email, don't ignore it. But don't panic either.

Ask:

1. Has this breach data been seen circulating online yet?
2. Is it searchable through services like Have I Been Pwned or DataBreach.com?

3. What kind of data was taken—passwords, SSNs, credit cards, or just emails?

Act:

- If the answer to #1 or #2 is yes, you're dealing with a **circulating breach.** That's your cue to act.
- If the data is very sensitive, like passwords or credit cards, you should act now even if the data is not visibly circulating.

Bottom Line

> Getting a breach notice doesn't always mean your data is in the wrong hands.
> It means you should figure out whether the breach is *disclosed* or *circulating.*

The real danger isn't the announcement. It's the circulation. That's when the bad guys stop guessing. And start using your data.

Call to Action: If you've received a breach notice recently and want to know whether it's circulating, or if you need to take action, ObscureIQ can help.