



When a Company's Data Breach Puts Your Information at Risk

You can do everything right online and still end up on a spreadsheet you never agreed to be part of. Data compromises hit a record 3,322 last year, according to the Identity Theft Resource Center — a 79% jump over five years.¹ The FTC logged over 1.1 million identity theft reports in 2024 alone, up nearly 10% from the year before.² Most of those cases didn't start with a mistake the victim made. They started with a company getting breached and a name, a Social Security number, or an account log-in landing somewhere it shouldn't.

Start With What You Can Control

Strong, unique passwords and app-based two-factor authentication still matter, and if you haven't already moved off text-message codes for your bank or brokerage login, that's worth doing this month. But no amount of personal diligence stops a retailer, a healthcare provider, or a vendor you've given any amount of information to from getting hacked. That's the uncomfortable truth behind most breach notices: they're not a reflection of your habits.

When the Notice First Arrives

This is where the real work happens. First, don't panic and don't ignore it — read what data was exposed, since a breached email address and a breached Social Security Number call for different responses. If financial or SSN data was involved, put a freeze on your credit with all three bureaus; it's free and can help prevent new accounts from being opened in your name. Change the password on the breached account and any account where you reused it (yes, even the ones you're sure are unrelated). Turn on transaction alerts for your bank and credit cards so you can be notified more quickly of potentially unauthorized activity.

Watch for the Second Wave

Unfortunately your leaked info can become a scammer's way in, and the breach notice itself becomes bait. Scammers know a breach is happening and send follow-up emails or texts pretending to be the breached company, asking you to "click here to enroll in your free monitoring" or "verify your account to prevent fraud." These messages can look identical to the legitimate ones. The safer move is to skip the link entirely and go directly to the company's website by typing the address yourself, then look for the breach information there. If you get a call claiming to be from the company's fraud department, hang up and call the number on your card or statement instead. A breach makes you a target twice, once for the original exposure and again for whoever tries to profit from your alarm.

Know What the Free Monitoring Actually Covers

Many breached companies offer a year or more of free credit monitoring, and it's worth signing up. Just go in with the right expectations. Credit monitoring typically watches for new accounts and hard inquiries tied to your SSN, but it won't necessarily catch every kind of misuse, and coverage varies by provider. Pairing it with a credit freeze and regular reviews of your bank and card statements can provide a broader oversight than relying on the monitoring service alone.

A breach notice in your inbox isn't a verdict on anything you did wrong. It's a prompt to act quickly and carefully. Knowing the right steps ahead of time makes that a lot less stressful when it happens.

To learn more about strategies that put you in control of your financial future, contact the office to schedule a time to talk.



FINANCIAL WATCH

¹Identity Theft Resource Center. "2025 Annual Data Breach Report." 2026, ITRC.org.

²Federal Trade Commission. "Consumer Sentinel Network Data Book 2024." 2025, FTC.gov.

The opinions expressed and material provided are for general information and should not be considered a solicitation for the purchase or sale of any security. The content is developed from sources believed to be providing accurate information.

Cetera Financial Group (Cetera) is a network of independent retail firms, including those that are members of FINRA/SIPC: Cetera Advisors LLC; Cetera Wealth Services, LLC (formerly known as Cetera Advisor Networks); Cetera Investment Services LLC (marketed as Cetera Financial Institutions or Cetera Investors); and Cetera Financial Specialists LLC. Entities registered as investment advisers with the Securities and Exchange Commission include Cetera Investment Management LLC and Cetera Investment Advisers LLC. Cetera's principal office is located at 655 W. Broadway, 11th Floor, San Diego, CA 92101.

Avantax Planning Partners, Inc. is an SEC registered investment adviser within the Aretec Group, Inc. (dba Cetera Holdings, an affiliate of Cetera). All the referenced entities are under common ownership.

Individuals affiliated with Cetera firms are either Registered Representatives who offer only brokerage services and receive transaction-based compensation (commissions), Investment Adviser Representatives who offer only investment advisory services and receive fees based on assets, or both Registered Representatives and Investment Adviser Representatives, who can offer both types of services.

This communication is designed to provide accurate and authoritative information on the subjects covered. It is not, however, intended to provide specific legal, tax, or other professional advice. For specific professional assistance, the services of an appropriate professional should be sought.

Some IRAs have contribution limitations and tax consequences for early withdrawals. For complete details, consult your tax advisor or attorney. For a comprehensive review of your personal situation, always consult with a tax or legal advisor. Neither Cetera Firms nor any of its representatives may give legal or tax advice.