MOVEIt breach impacts Genworth, CalPERS as data for 3.2 million exposed

By Bill Toulas

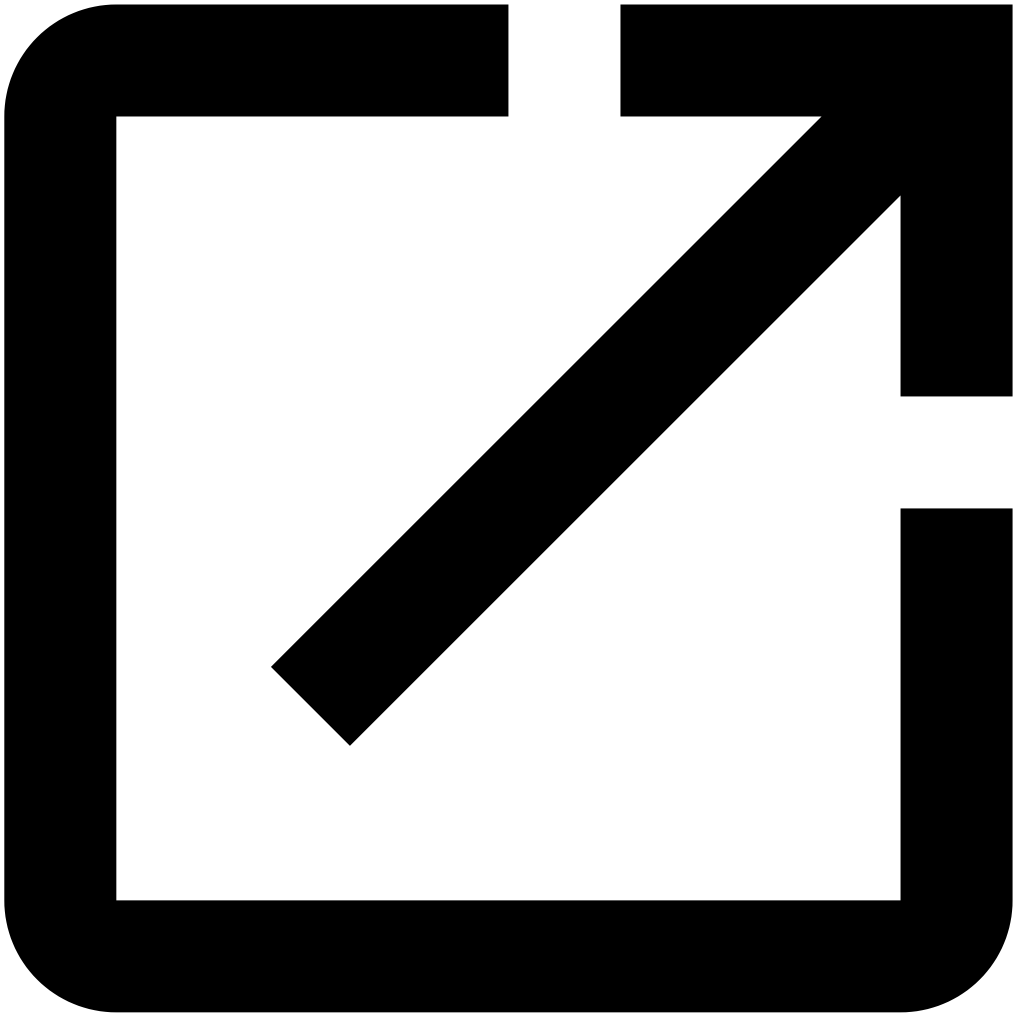
Published: 2023-06-23 · Archived: 2026-04-05 12:58:50 UTC

PBI Research Services (PBI) has suffered a data breach with three clients disclosing that the data for 4.75 million people was stolen in the recent MOVEit Transfer data-theft attacks.

These attacks started on May 27th , 2023, when the Clop ransomware gang began exploiting a MOVEit Transfer zero-day vulnerability to allegedly steal data from hundreds of companies.

Over the past week, the Clop gang began extorting companies by slowly listing impacted organizations on its data leak site as they attempt to pressure victims to pay a ransom demand.


DIE LINKE.
0:00



According to three different disclosures from PBI clients, millions of customers have had their sensitive data exposed in these attacks. However, this number may increase as other companies make further disclosures.

The first impacted entity is Genworth Financial, a Virginia-based life insurance services provider.

In a MOVEit Security Event notice published on their website, Genworth says PBI informed them of the security breach on June 16, 2023, and subsequently verified that customers' personal data was stolen.

The firm estimates that the data breach impacted between 2.5 and 2.7 million individuals who are either its customers (insurance, annuity, long-term care) or working for them as insurance agents.

The exposed data includes the following:

- Full name
- Date of birth
- Social security number
- Zip code
- State of residence
- Policy number
- Agent ID (for agents)

Genworth says this attack did not impact its own systems and network or affected its business operations, as it does not use the MOVEit or GoAnywhere products.

Affected individuals will receive notices of a data breach in the coming weeks, which will contain instructions on enrolling for free-of-charge credit monitoring and identity theft protection services.

The second firm impacted by the PBI breach is Wilton Reassurance, a New York-based insurance provider, which reports that 1,482,490 of its customers had data stolen.

As reported to the Office of the Maine Attorney General, the exposed information includes customers' names and social security numbers.

Although a sample of a data breach notification letter has not been uploaded to Maine's portal yet, Wilton Reassurance has informed that they will provide 12 months of free identity theft protection and credit monitoring services through Kroll to impacted individuals.

The third company impacted by PBI's data breach is CalPERS (California Public Employees' Retirement System), the largest public pension fund in the US, which is now informing retirees and beneficiaries about the event.

In a notice to its website, CalPERS says it responded to the situation immediately after learning about the breach and took actions to secure its members' benefits and data by strengthening its data management protocols that pertain to working with contractors.

The agency says approximately 769,000 of its members were impacted by the security incident, who will all receive notification letters with detailed information on how to access two years of free credit monitoring service through Experian.

At the time of writing this, PBI Research Services has not been listed on Clop's data leak site. While this could mean that the company is negotiating with the threat actors not to release data, it could also mean that Clop has not begun extorting the organization yet.

BleepingComputer has contacted PBI to comment on the situation, but we have not heard back by publication.

Update 6/24 - A PBI spokesperson has sent BleepingComputer the following comment:

> PBI Research Services uses Progress Software’s MOVEit file transfer application with a number of clients. At the end of May, Progress Software identified a zero-day vulnerability in the MOVEit software that was actively being

> exploited by cyber criminals.
>
> PBI promptly patched its instance of MOVEit, assembled a team of cybersecurity and privacy specialists, notified federal law enforcement and contacted potentially impacted clients.
>
> The cyber criminals did not gain access to PBI's other systems – access was only gained to the MOVEit administrative portal subject to the vulnerability.
>
> PBI is working directly with impacted clients to identify impacted consumers and develop notice plans.

Source: https://www.bleepingcomputer.com/news/security/moveit-breach-impacts-genworth-calpers-as-data-for-32-million-exposed/