POLSINELLI

Publications

October 10, 2025 • Updates

$19M in Settlements Underscore Cybersecurity Risks for TPAs and Insurers

Key Takeaways

- Two recent data breach class action settlements involving third party administrators and their insurer co-defendants have resulted in nearly $20 million in combined payments.
- The class actions stem from two large-scale data breaches in 2023 and 2024 that affected more than 3 million individuals across the U.S. and triggered consolidated litigation focused on alleged failures to implement basic cybersecurity safeguards.
- These cases signal growing litigation risk for TPAs and insurers: even without a finding of wrongdoing, data security lapses can lead to substantial legal and financial exposure.

In two separate but related actions, third party administrators (TPAs) and their insurance business partners agreed to substantial settlements to resolve allegations that they failed to adequately safeguard sensitive data from cyberattacks. Though neither case involved a finding of fault, both spotlight a growing trend: plaintiffs and regulators are treating basic cybersecurity failures as actionable — and expensive.

For TPAs and insurers, the message is clear: even without an admission of wrongdoing, perceived data security missteps can carry steep legal and financial consequences.

Two Breaches, Two Settlements: A Closer Look

In the first case, which settled in September 2025, a TPA serving self-funded employers and its co-defendant insurers agreed to pay $13.75 million to resolve claims tied to a 2023 data breach. The incident allegedly compromised the protected health information (PHI) of more than 2.5 million individuals, including a subclass of California residents. The TPA and its co-defendants were named in 13 class action lawsuits over the data breach, which were consolidated into a single action in the U.S. District Court for the Northern District of Texas, Dallas Division. The consolidated lawsuit alleged the TPA and its co-defendants failed to implement reasonable cybersecurity measures to protect sensitive data and information. Although they denied liability, the TPA and insurers agreed to settle.

Related People

- Steven L. Imber
- Justin T. Liby
- Jennifer L. Osborn
- Zachary R. Dyer
- Pavel (Pasha) A. Sternberg

Related Capabilities

- Third Party Administrator (TPA) Licensing & Compliance Services
- Insurance
- Privacy & Cybersecurity
- Data Breach & Incident Response

The second settlement, finalized in October 2025, resolved a Texas class action lawsuit involving a 2024 data breach that allegedly impacted the personal and health information of more than 800,000 policyholders' records held by a Texas-based TPA. The suit alleged that the TPA and its insurer partners — in failing to implement reasonable cybersecurity measures — failed to prevent a cyberattack that exposed names, health insurance information, Social Security numbers and financial account details. As with the earlier case, the defendants did not admit liability but agreed to a $6 million settlement.

Why This Matters for TPAs and Insurers

Together, these settlements reinforce a growing reality: organizations that handle large volumes of sensitive data — especially TPAs and insurers — must treat cybersecurity as a core compliance function, not just an IT issue. As plaintiffs and regulators continue to focus on what constitutes "reasonable" protections, failure to meet that standard can expose companies to costly class actions, regardless of intent or admission of fault.

Companies in all industry sectors are struggling to keep pace with cybersecurity threats, but for TPAs in particular, these cases highlight the need to regularly review internal data security practices, strengthen breach response protocols and evaluate third-party risk. The cost of inaction isn't just theoretical — it's reputational, regulatory and increasingly financial.

For More Information on Our TPA and Privacy and Cybersecurity Compliance Teams

Polsinelli's TPA team provides a number of services to TPAs including licensing, regulatory and compliance services, assistance with audits, government examinations and investigations, drafting administrative services agreements and a myriad of other services. Our TPA team includes former state insurance regulators and former in-house counsel for TPAs, which provide our TPA clients with significant experience to help navigate complex insurance regulatory challenges efficiently.

By leveraging its extensive experience representing TPAs, our TPA team helps clients avoid the learning curve and related cost implications that can be experienced by working with companies or attorneys less familiar with the insurance regulatory and compliance needs of TPAs.

Polsinelli's Data Privacy & Cybersecurity team has significant experience with navigating the constantly evolving data privacy law landscape. Our interdisciplinary approach encompasses all data and network security aspects before and after an incident — we assist organizations in preparing for data incidents as well as providing comprehensive assistance when an incident occurs.

For questions regarding this e-alert, other TPA regulatory and compliance matters, and privacy or cybersecurity matters, please contact one of the authors, a member of Polsinelli's TPA or Privacy and Cybersecurity Compliance teams or your Polsinelli attorney.