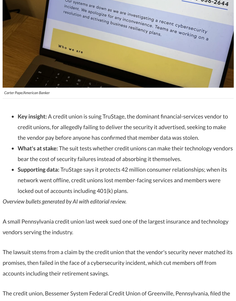
CYBER SECURITY

Credit union sues TruStage over cybersecurity incident

By Carter Pape

Published July 23, 2024, 4:41 p.m. EDT | Updated July 23, 2024, 9:08 p.m. EDT

8 Min Read



Carter Pape/American Banker

- **Key insight:** A credit union is suing TruStage, the dominant financial-services vendor to credit unions, for allegedly failing to deliver the security it advertised, seeking to make the vendor pay before anyone has confirmed that member data was stolen.
- **What's at stake:** The suit tests whether credit unions can make their technology vendors bear the cost of security failures instead of absorbing it themselves.
- **Supporting data:** TruStage says it protects 42 million consumer relationships; when its network went offline, credit unions lost member-facing services and members were locked out of accounts including 401(k) plans.

Overview bullets generated by AI with editorial review.

A small Pennsylvania credit union last week sued one of the largest insurance and technology vendors serving the industry.

The lawsuit stems from a claim by the credit union that the vendor's security never matched its promises, then failed in the face of a cybersecurity incident, which cut members off from accounts including their retirement savings.

The credit union, Bessemer System Federal Credit Union of Greenville, Pennsylvania, filed the proposed class action July 17 against TruStage Financial Group, the Madison, Wisconsin, company formerly known as CUNA Mutual Group.

The suit came two days after TruStage disclosed that it had taken its network offline to deal with what it described in a statement as a cybersecurity incident.

TruStage is among the most widely used insurance and financial-services providers in the credit union industry. It enables credit unions to offer life and auto insurance and retirement accounts.

The company says 93% of U.S. credit unions do business with it. On its website, it says it protects 42 million consumer relationships.

When its systems went dark last week, credit unions lost some of those services, and members got locked out of accounts including 401(k) plans.

Now, one of those affected credit unions wants TruStage to pay for the damage, although it hasn't said what exactly that damage is. Bessemer is suing on behalf of every U.S. credit union that handed TruStage confidential data and got caught up in the incident.

The complaint lodges a single claim of negligence and seeks damages, repayment of the money credit unions spent on what it calls deficient services and reimbursement for breach-related costs.

Bessemer's negligence theory is well-worn but hard to win, even if the credit union may clear a hurdle that sinks many data-breach suits, according to experts who commented on the case.

Read more:

- Four factors that drove banks' blowout 2Q performance
- Banks face a dilemma: More loan growth or better margins?
- The top-performing 20 public banks with under $2B of assets in 2025
- 'The data has to be perfect': BofA CEO Moynihan on AI

What TruStage has said, and what it hasn't

In a July 15 statement, TruStage said it "recently identified a cybersecurity incident affecting its environment and immediately activated its incident response and recovery protocols."

The company also "engaged external cybersecurity experts to support containment, remediation and recovery efforts," according to the statement.

"Our systems are down as we are investigating a recent cybersecurity incident," a notice on its website at the time read.

On a customer service FAQ page, the company said it "proactively shut down our network and systems." TruStage said on that page it would be "premature to draw conclusions about the scope or impact of the incident, including whether any data may have been accessed."

With respect to when members would be able to reach their 401(k) accounts, it said in the FAQ only that it was "working diligently to restore systems."

As of midday Tuesday, the page said customers "may experience difficulty accessing account information, completing transactions or submitting requests online."

TruStage has not said how intruders got in or who was behind the incident. It has confirmed no ransom demand and named no attacker.

The company identified the incident on July 11, four days before it disclosed it publicly, and had not seen "any threat actor activity" since it first became aware of it, Barclay Pollak, a TruStage spokesperson, told American Banker.

Pollak declined to address Bessemer's allegations, saying TruStage does not comment on pending litigation.

A vendor's promises against its performance

Bessemer says TruStage's real security did not match what it promised the credit unions that hired it.

TruStage's privacy policy says the company "maintains physical, technological and administrative safeguards to protect your personal information and prevent unauthorized or accidental use, access, or loss."

A separate document TruStage gives credit unions to vet its security, its "2025 security practices," represented that the company backed up data on a regular schedule and tested at least once a year that "critical business processes can be recovered timely," according to the complaint.

One or more of those representations "were not accurate when made," the complaint alleges.

Since July 15, credit unions and their members have had "limited or no access" to TruStage accounts, "including employee retirement accounts such as 401(k) plans," and "normal business operations with TruStage have come to a halt," according to the July 17 complaint.

Claims also stalled for auto-loan gap coverage, mechanical-repair coverage and payment-protection products, which are the kinds of add-ons credit unions sell through TruStage.

"Pursuing a legal claim is the most powerful tool a credit union has to protect its members and obtain compensation from culpable third-party vendors," said Joy Peterson, Bessemer's chief executive, in a statement announcing the suit.

Charles Nerko, an attorney for the credit union, said in the same statement that every credit union "is entitled to vendors whose security practices match their security promises."

The complaint is thin on the specifics of the breach itself, reflecting the lack of specifics TruStage has provided. The complaint alleges "on information and belief" (a legal term for a claim a party believes is true but cannot yet prove) that unauthorized outsiders reached TruStage's systems.

The complaint identifies no stolen data and no attacker. It also does not spell out what Bessemer itself lost, describing the disruption for credit unions as a class.

Nerko told American Banker the credit union's investigation is continuing and that he expects to file an amended complaint as more about the incident comes to light. He also said his firm has heard from many other credit unions caught in the outage — a sign the fallout reaches beyond Bessemer.

Not Bessemer's first fight with a vendor

Bessemer has taken a technology vendor to court before. In 2019, it sued Fiserv, which runs the back-end infrastructure called core systems that many banks and credit unions use to process accounts.

In that lawsuit, Bessemer accused Fiserv of what its complaint called "baffling" security lapses and billing errors. It settled the case on confidential terms in 2024.

Weeks after that suit ended, Bessemer paid its members a one-time special dividend of $100 each, saying the payout let members "share in our credit union's recent successes," according to a June 2024 report in the trade publication CU Today.

An early test of vendor liability

Bessemer, which sued TruStage before anyone confirmed data got stolen, is pinning its negligence claim on the disruption and the risk (rather than proof) that members' information got exposed.

A claim like this starts with the contract, according to Matthew Wolfe, a data-breach class-action litigator at Shook, Hardy & Bacon. Wolfe is not connected to the case.

"The first place I'd go is the contract between the vendor and the customer," he told American Banker. "If it addresses data security, that gives you a fairly clean answer."

If it doesn't, "you could still make a claim on the grounds of common law," he said, arguing that "the vendor had a duty to exercise reasonable security measures."

That common-law route is the one Bessemer has taken.

"This isn't a new or novel theory," Stephen Reynolds, a data-security litigation partner at McDermott Will & Schulte who is also independent of the suit, told American Banker.

Pleading negligence over a vendor's security representations "gives class action plaintiffs a way to pursue recovery outside contract, but courts rarely make that path easy," he said.

Reynolds pointed to two hurdles. First, courts often dismiss tort claims between businesses under the economic loss doctrine, which "generally bars recovery for purely financial losses where the parties' relationship is governed by contract," he said.

Second, courts "tend to be cautious about recognizing a broad common-law duty for third-party software vendors that would go beyond their express contractual commitments," he said.

But TruStage's own security assurances (the documents at the center of Bessemer's complaint) could serve as the big evidence against it.

"In the course of litigation, the vendor's own security measures may help establish the standard of care it allegedly failed to meet," Reynolds said.

One question has sunk many data-breach cases: Can the plaintiff show a concrete enough injury to sue in federal court when no theft is confirmed? Reynolds said a credit union facing this question stands on firmer ground than an individual consumer would.

Institutional plaintiffs often face fewer hurdles getting heard in court compared to individual consumer data-breach plaintiffs, he said. Consumer cases often fail when the only claimed harm is a speculative future risk of identity theft.

An institution, by contrast, "can point to direct and immediate operational losses, such as lost transaction revenue, staffing costs during downtime, remediation expenses, and fees paid for services that were not provided," he said.

"Those concrete monetary harms are more likely to satisfy the requirement of an actual injury," Reynolds said.

Carter Pape
Technology Reporter

Carter Pape has covered cybersecurity, financial crime and emerging technology for American Banker since January 2022.Pape, reporting from... Read full bio

CYBER SECURITY LITIGATION CREDIT UNIONS RISK MANAGEMENT VENDOR MANAGEMENT TECHNOLOGY