

When a Critical Vendor Goes Dark, Is Your FI Ready?

By Steve Fochler

In July, TruStage, a vendor serving credit unions and their members, [shut its network down](#) after a cybersecurity incident. Financial institutions were left dealing with outages that slowed processes, angered consumers, and lost revenue.

That's the uncomfortable truth about third-party risk. The vendor's problem becomes your problem the moment its systems go dark. What matters is whether your institution is prepared with a plan in case of a vendor outage.

How a Vendor Outage Spreads Risk Across Your FI

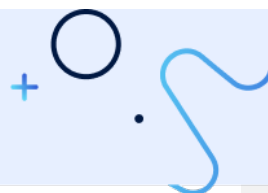
A third-party outage rarely stays contained to the vendor's own systems. It multiplies risk across the organization, and the exposure dominos across risk areas:

- **Financial:** A vendor-supported product or service going down means lost revenue for as long as the outage lasts. In the case of TruStage, it meant anything from delayed loan closings to lost ancillary product revenue.
- **Compliance:** Depending on the regulator involved, an incident can trigger notification obligations before a vendor has even finished its investigation. The assessment should be based on what you know, not what the vendor eventually discloses.
- **Operational:** Staff lose system access, customers can't complete routine transactions, and the organization runs on manual workarounds until service returns, shaping how customers experience the institution for as long as the disruption continues.

The scale of this exposure isn't hypothetical. More than half of financial organizations [reported a third-party cyber incident in the past year](#), up from the year before. When a vendor serves a large share of an industry while holding sensitive data across many institutions, one incident stops being a single company's problem — it becomes a sector-wide exposure.

How to Respond While the Vendor is Down

When a critical vendor goes down, the priority is protecting consumers from harm while keeping a clean, defensible record of everything that happens. That starts with logging every request as it comes in, whether it's a claim, an enrollment, or a change order, even if you can't process it until



the vendor is back online. The date a consumer reaches out should count as the official date of their request, protecting them from being penalized for downtime that isn't their fault. Extend and document any time-sensitive deadline that could lapse during the outage, and route all vendor communication through a single designated owner so nothing falls through the cracks.

From there, the work is manual: document each request, assign it a reference number, and hold it for batch submission once systems are restored. If a claim depends on confirmation that hasn't happened yet, don't close it out or waive anything tied to it. If the delay could otherwise cost a consumer something, such as a late fee or a paused benefit, hold that penalty until the vendor is back online.

On the regulatory side, don't wait for the vendor's investigation to conclude before assessing your own notification obligations. Document that reasoning either way, and loop in compliance and counsel early.

Once the vendor confirms restoration, the work shifts to reconciliation: submit logged requests in batch while preserving original dates, check the manual log against the vendor's confirmations, lift temporary holds, and correct records as needed. Then close the incident, capture what you learned, and update the vendor's continuity plan accordingly.

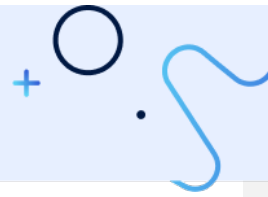
How Fis Can Prepare Before the Next Outage

The best time to think through vendor outage response is before you need it, and contract management is where that starts. Notification timelines matter here. A contract that only promises notice "as soon as reasonably practicable" gives an institution far less to work with than one that specifies a number of hours. Negotiate clear expectations for downtime and breach liability, and require the vendor to keep you updated during an incident so you're not forced to piece things together from the news.

A few habits strengthen that foundation regardless of what any single vendor's investigation eventually finds:

- Documenting what happened in real time, including who told whom what and when, holds up far better under regulatory or legal scrutiny than reconstructing events from memory weeks later.
- A dedicated incident response team that already knows its roles moves faster than one figuring out who's in charge while a vendor is still down.

Commented [GR1]: Add product link



- A [tabletop exercise](#) built specifically around a critical vendor going dark with no explanation surfaces gaps that a general disaster-recovery test won't catch. This is especially true when it extends into a functional test with a key service provider, such as a PR firm or cyber insurance carrier.

A vendor's bad day is out of your control. How ready you are for it isn't.

About Ncontracts

Ncontracts provides integrated risk management, compliance, and third-party risk management solutions to over 5,500 organizations worldwide, including 4,500 U.S. financial institutions, mortgage companies, and fintechs. The flagship Ncontracts IRM suite combines AI-powered software with expert services, helping financial institutions streamline risk, compliance, and vendor management through an intuitive, cloud-based platform. Ncontracts' Venminder solution is trusted by enterprise financial companies and other large organizations to strategically manage third-party risk across the entire vendor lifecycle.

Visit www.ncontracts.com or follow the company on [LinkedIn](#) and [X](#) for more information.