DATA SHEET

Vendor Breach Monitoring

Continuous, managed breach monitoring for vendor risk

Vendor breach response is often reactive and hard to prove.

Financial firms are under increasing pressure to identify vendor-related data breaches quickly, assess exposure, and notify impacted customers within strict regulatory timelines. The SEC's amended Regulation S-P establishes a 30-day outer limit for customer notification following a breach, while vendors are required to report incidents within 72 hours. Compliance deadlines are approaching for both larger and smaller firms.

Yet many organizations still rely on vendors to self-report incidents. That reactive approach, combined with manual monitoring and fragmented workflows, creates real risk: missed alerts, delayed assessments, incomplete documentation, and gaps in the audit trail.

Vendors must protect the data. But firms must prove they can, ensure they do, and act if they do not.

Move from reactive to proactive breach detection

Smarsh Vendor Breach Monitoring is an add-on to Smarsh Vendor Risk Management that continuously monitors your vendor ecosystem for data breaches using a third-party intelligence feed. When a breach is detected, Smarsh matches the breached vendor against each client's VRM inventory and initiates a structured, auditable response workflow.

Smarsh Managed Services handles detection, notification, vendor assessment, and reporting—helping firms move from reactive vendor self-reporting to proactive breach readiness.

No client data is ever shared with the breach monitoring provider.

What this means for you

Strengthen compliance readiness

Continuously monitor vendors for breach activity and support Reg S-P readiness without building a manual monitoring process from scratch.

Reduce reliance on vendor self-reporting

Layer independent breach intelligence on top of your vendor risk workflow so your team is not waiting for vendors to disclose incidents.

Streamline breach response

Smarsh Managed Services helps coordinate detection, client notification, vendor assessment, and reporting—reducing the need for new internal workflows.

Create a defensible audit trail

Every breach alert, notification, and vendor assessment response is documented within VRM to support regulatory exams and internal oversight.

Build on your existing VRM program

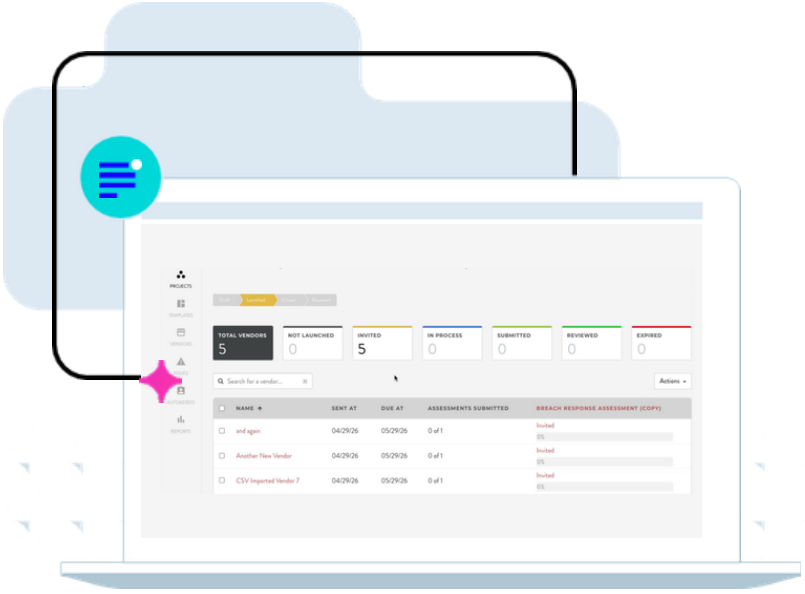
Vendor Breach Monitoring is layered onto your existing Smarsh VRM vendor inventory, helping avoid duplicate systems, separate logins, or re-keying vendor data.

How It Works

Vendor Breach Monitoring turns breach intelligence into action through a managed, auditable workflow—helping firms detect impacted vendors, notify stakeholders, assess vendor response, and document every step within Smarsh VRM.

1. **Detection & Review**
   Smarsh receives a breach alert from a third-party intelligence feed and matches the breached vendor against each client's VRM inventory.

2. **Client Notification**
   Smarsh sends an email notification identifying the breached vendor and providing available breach details.



3. **Vendor Assessment**
   Smarsh sends a breach assessment questionnaire directly to the breached vendor.

4. **Reporting**
   All breach responses are documented within VRM for audit and regulatory requirements.

Why choose Smarsh?

- Smarsh helps firms translate complex compliance obligations into operational workflows.
- Our team reduces the burden on internal resources by managing key response steps.
- Breach monitoring works within your existing Smarsh vendor risk program.
- Smarsh brings deep experience supporting regulated firms with oversight, governance, and audit readiness.

To learn more, contact your Smarsh representative or visit our VRM webpage at: https://www.smarsh.com/smb/vendor-risk-management/