VENDOR RISK CHECKLIST

8 questions to ask any collections partner

When a collections or revenue cycle vendor is breached, the regulators, the headlines and the angry customers come to you. Using a partner doesn't move that responsibility.

Use these eight questions in your next vendor review. A mature partner answers each one with documents in minutes, not with promises. Check the box only when you've seen the evidence.

> **Why this matters now.** The CFPB expects supervised companies to oversee their service providers for compliance with consumer financial law (Compliance Bulletin 2016-02). Federal banking agencies expect the same in the 2023 Interagency Guidance on Third-Party Relationships. A September 2026 proposal would replace that guidance with a more risk-tailored approach, and it keeps the core point: you remain responsible for work done on your behalf.

1 ☐ Can you show current independent audit reports?

ASK FOR

- Latest SOC 2 Type II report and its date range
- PCI DSS attestation of compliance if they take card payments
- Bridge letter if the report period has ended

RED FLAGS

- "We're compliant" with no report
- A SOC 2 Type I only, or a report more than a year old
- Certificates for the hosting provider, not the vendor

2 ☐ Where does our data live, and how is it moved?

ASK FOR

- Hosting locations, including whether data or work goes offshore
- File transfer method (SFTP with encryption, or API)
- Encryption at rest and in transit

RED FLAGS

- Account files sent by email or plain FTP
- "We'd have to check" on data location

3 ☐ Who can touch our accounts, and how do you control it?

ASK FOR

- Background screening policy for staff with data access
- Multi-factor authentication for remote and privileged access
- Least-privilege roles and quarterly access reviews

RED FLAGS

- Shared logins or generic admin accounts
- No record of when access was last reviewed

4 ☐ How is your network built and watched?

ASK FOR

- A network diagram showing segmentation of client data
- Intrusion detection and log monitoring, and who watches it
- Most recent third-party penetration test summary

RED FLAGS

- A flat network with everything on one segment
- No penetration test in the last 12 months

5 ☐ When did you last restore from backup, and can we see it?

ASK FOR

- Backup schedule and where copies are kept
- Date and result of the last disaster recovery test
- Recovery time and recovery point targets

RED FLAGS

- Backups that have never been test-restored
- A DR plan that hasn't been exercised this year

6 ☐ What happens in the first 24 hours of an incident?

ASK FOR

- The incident response plan and who owns it
- When and how you will be notified, in writing in the contract
- Date of the last tabletop exercise

RED FLAGS

- No contractual notification window
- A plan that names nobody

7 ☐ How do you prove every consumer contact followed the rules?

ASK FOR

- Call recording and how much of it is reviewed
- How consent and opt-outs for text and email are captured and honored
- Contact limits built into the dialer (Regulation F, 12 CFR 1006.14)
- Complaint volume and how complaints are resolved

RED FLAGS

- Opt-outs handled by hand, one channel at a time
- No complaint data they're willing to share

8 ☐ Who else touches our data?

ASK FOR

- A list of subcontractors and fourth parties with data access
- How the vendor reviews them, and how often
- For patient data, a signed HIPAA business associate agreement

RED FLAGS

- Unknown subcontractors (letter vendors, dialers, payment processors)
- No right for you to audit or to be told about changes

SCORING

How did your partner do?

8 of 8
Evidence on everything. Keep monitoring yearly.

5 to 7
Get dates and owners for the gaps, in writing.

4 or fewer
Escalate to your risk team before renewal.

Review log

Vendor	Date	Score	Gaps and owner

TSI'S ANSWERS

How TSI answers these questions

Question	TSI evidence
1. Independent audits	SOC 2 Type II, examined annually; PCI DSS service provider attestation
2. Data location and transfer	Client data kept in the United States; encrypted SFTP or API transfers; encryption at rest and in transit
3 and 4. Access and network	Background screening, multi-factor authentication for privileged access, segmented network with continuous monitoring, annual third-party penetration testing
5 and 6. Recovery and incidents	Business continuity and disaster recovery plans tested annually; documented incident response with client notification
7. Consumer contact	Call recording, consent tracking, and a 99.997% complaint-free contact rate
8. Healthcare data	HIPAA business associate agreements and safeguards

> **See it live.** Ask for a 20-minute security walkthrough and we'll show the documents behind each answer. Visit tsico.com to reach our team.

Sources

- CFPB Compliance Bulletin and Policy Guidance 2016-02, Service Providers.
- FDIC, FRB and OCC, Interagency Guidance on Third-Party Relationships: Risk Management, 88 FR 37920 (June 9, 2023).
- FDIC, FRB, NCUA and OCC, Proposed Third-Party Risk Management Guidance, 91 FR 58536 (Sept 15, 2026).
- Regulation F, 12 CFR part 1006 (eCFR).

General information, not legal advice. TSI has served clients since 1970. © 2026 Transworld Systems Inc.