Due diligence checklist: GLBA Safeguards

Gramm-Leach-Bliley Act: Interagency Guidelines Establishing Information Security Standards and the FTC Safeguards Rule. Federal banking agencies and the FTC, the United States.

Regime	GLBA Safeguards
Regulator	Federal banking agencies and the FTC
Country	the United States
Regulator's page	https://www.ftc.gov/business-guidance/resources/ftc-safeguards-rule-what-your-business-needs-know
Prepared	9 November 2026
Current version	https://www.vederca.com/market-scan/due-diligence/us-glba

What it is

Service providers that handle customer information are overseen and bound to safeguard it.

Who it applies to

Applies to every financial institution in the United States.

What to ask a vendor, and the evidence to request

#	Ask the vendor for	Evidence to request	Received
1	Contractual safeguards for customer information, including encryption and access control	A description of the security controls, the most recent control testing or penetration test summary, and the policies for vulnerability, change and access management.	
2	An incident response capability and notice of unauthorised access to customer information	The incident notification clause and procedure: what counts as an incident, who is told, within what time, and a record of a past notification if one exists.	

In every case

- A named contact at the vendor responsible for this regime, and how the vendor tracks changes to it.
- Which named customers the vendor already serves under this regime, as references you may call.

This checklist is a starting point for a procurement team, not legal advice. Read it with the regulator's own page, your institution's policies and your legal and risk teams; the regime may have changed since the date on this document.