Verillian for Financial services

GLBA, SOX, SR 11–7

Model risk management expects a record of what models did. Verillian gives risk and compliance functions tamper-evident evidence and policy enforcement across every AI tool in use.

$6.08M

Average cost of a data breach in financial services, second only to healthcare. IBM Cost of a Data Breach Report, 2024.

WHAT'S AT STAKE

When AI tools operate across the institution with no enforced policy and no tamper-evident record, sensitive customer and account data can leave the boundary unredacted and unlogged, with no defensible account of what any model did. Examiners under SR 11-7, SOX, and GLBA expect a reconstructable record of model behavior; without one, the institution carries the full breach and penalty exposure.

HOW VERILLIAN ANSWERS

Tamper-evident model evidence for SR 11-7	Every AI interaction is signed on the device and hash-chained into an append-only record, the construction used in financial ledgers, giving model risk management a non-repudiable account of what each model did and when.
GLBA data protection at the boundary	Sensitive-data detection redacts or blocks SSNs, account numbers, and other configured PCI and PII types before a request leaves the device, so customer financial data does not reach an outside provider unredacted.
Enforcement across every AI tool, including shadow AI	A sentinel governs any tool that speaks HTTPS to a provider, enforcing deny-by-default policy at execution and surfacing shadow AI and unsanctioned tool calls across the fleet.
Fail closed, with audit retention for examination	If policy is missing or the audit pipeline fails, AI traffic stops. Ciphertext is held under the institution's own key on a zero-knowledge server, with retention aligned to the applicable framework.

Source: https://www.ibm.com/think/insights/cost-of-a-data-breach-2024-financial-industry