TripleKey

FOR BANKS AND CREDIT UNIONS

The Banking Risk Brief

Seeing the software supply chain risk inside every vendor your bank depends on.

Banks are examined on third party risk but breached through vendor code. This brief maps the gap between the two, the breach record of 2025 and 2026 that proved it, the AI exposure entering vendor software, and how banks use continuous code level evidence to oversee every vendor in the portfolio.

For CEOs, CFOs, CISOs, chief risk and compliance officers, and board and audit committees at banks and credit unions.

JUNE 2026

EXECUTIVE SUMMARY

Why this brief, and why now

Banking runs on software the bank did not write. Core processors, digital banking platforms, lending and account opening tools, fraud engines, treasury systems, and a growing roster of fintech partners all sit inside the same regulated perimeter. Each vendor brings its own open source dependencies, its own contributors, and its own unpatched code, and the signals that actually predict loss live inside that software, changing every day.

The numbers tell the story. Third party involvement in breaches doubled in a single year, from 15 percent to 30 percent of all breaches (Verizon DBIR 2025). Supply chain compromise costs $4.91 million per incident and takes 267 days to identify and contain, the longest of any attack vector (IBM Cost of a Data Breach 2025). And in August 2025, a single vendor compromise cascaded into data breaches at more than 70 banks and credit unions at once.

This brief is built for bank leadership. It maps the oversight gap in third party risk today, what the 2025 and 2026 breach record means for the bank, the AI exposure entering vendor code, the examiner pressure stack, the maturity curve, and the ten questions a board should ask this quarter.

THE THESIS IN THREE LINES

- **Vendor software risk is now a banking board issue.**
  The highest profile banking breaches of 2025 and 2026 did not start inside the banks. They started inside vendor software, and regulators hold the bank accountable either way.
- **A SOC 2 in a folder is not visibility.**
  Point in time attestations prove that controls existed on one day. Examiners, boards, and customers now expect continuous evidence of what is inside the software the bank depends on.
- **AI has raised the stakes on both sides.**
  Attackers are using AI to scale fraud and intrusion, while vendors ship AI generated code into bank facing systems faster than anyone reviews it.

THE OVERSIGHT GAP

Three places the current model leaks risk

01 Questionnaires expire on submission

A SOC 2, a completed questionnaire, or an ISO 27001 certificate describes the day it was issued, not the day the breach happens. Roughly 60 percent of breaches involved exploiting a known vulnerability for which a patch was already available (Verizon DBIR 2025). That is a posture decay problem, and no annual artifact can detect it.

02 Aggregation risk is invisible

A small number of processors and platform vendors serve thousands of institutions, so one upstream compromise arrives at many banks at once. In September 2025, CISA issued an emergency alert over Shai-Hulud, a self replicating npm worm that compromised more than 500 packages; a second wave in November backdoored roughly 796 more (CISA; Cloud Security Alliance). Without a portfolio wide view of what is inside vendor software, the accumulation only surfaces when the notification letters arrive.

03 Exam evidence lacks code

The 2023 Interagency Guidance holds the bank, not the vendor, accountable for ongoing monitoring of third party relationships. When a vendor breach lands, the bank needs certainty about what software was running, which dependencies were in place, and when warning signs first appeared. That record usually does not exist, and supply chain breaches already take 267 days to identify and contain, the longest of any vector (IBM 2025).

30%
of breaches now involve a third party, double the prior year
VERIZON DBIR 2025

$4.91M
cost per supply chain incident, 267 days to contain
IBM 2025

$5.56M
average breach cost in financial services, second only to healthcare
IBM 2025

48,185
new CVEs published in 2025, roughly 132 per day
NVD / NIST

BREACH REPORT · 2025 TO 2026

The breaches came through the vendors

The defining banking security stories of the past 18 months share one shape. The bank's own perimeter held. The software and vendors it depends on did not. Incident details below come from company notification letters and state regulator filings, as reported by American Banker and PYMNTS.

70+
banks and credit unions breached through one vendor in a single incident
REGULATOR FILINGS

13.1M
individuals in the Prosper Marketplace breach, the year's largest in financial services
COMPANY NOTICE

5.8M
consumers exposed via 700Credit, reached through a vendor's vendor
COMPANY NOTICE

1,251
entities hit by supply chain breaches in 2025, up from 660
ITRC 2025

- **One vendor, seventy institutions**
  Ransomware entered Marquis Software, a marketing and compliance vendor to community banks, through a known VPN vulnerability (CVE-2024-40766). More than 70 banks and credit unions and at least 400,000 consumers were affected, and the institutions carried the notifications, the filings, and the customer calls.
- **Fourth party risk is now on the record**
  Attackers reached 700Credit by first compromising a partner of the vendor, then using exposed credentials and an API flaw to scrape data on roughly 5.8 million consumers. TransUnion, breached through a third party support application in July 2025, showed that even the firms that score risk for banks get hit through their own vendors.
- **The bank's own controls never failed**
  Western Alliance Bank disclosed that a zero day in third party file transfer software exposed personal and financial data of roughly 22,000 customers. Its own perimeter was never touched. The software it bought was the breach.
- **Concentration surfaced again in April 2026**
  Citizens Bank and Frost Bank both notified customers after a breach at a single shared third party vendor. One compromise, two household name institutions, and the same lesson: vendor concentration means one event surfaces at many banks at once.

EMERGING RISK · AI ON BOTH SIDES

AI is now on both sides of the breach

01 AI as the attacker

About 1 in 6 breaches in 2025 involved an AI driven attack, averaging $4.49 million per incident (IBM 2025). Voice cloning lets attackers impersonate executives and vendors on the phone with audio sampled from earnings calls, and AI enabled fraud losses in the United States are projected to reach $40 billion by 2027 (Deloitte Center for Financial Services).

02 AI inside the software you buy

Roughly three quarters of developers report using or planning to use AI coding tools (Stack Overflow Developer Survey), so your vendors ship AI generated code into bank facing systems, and nothing in a questionnaire captures it. About one in five packages recommended by AI coding models does not exist, an attack path researchers named slopsquatting (USENIX Security 2025), and the Shai-Hulud npm worm demonstrated that malicious dependencies can spread autonomously through the same ecosystems AI tools draw from (CISA, September 2025).

03 AI inside the bank

One in five organizations reported a breach tied to shadow AI, employee use of unsanctioned AI tools, and those breaches cost roughly $670,000 more on average (IBM 2025). Examiners have started asking AI governance questions in the same breath as third party risk questions, because the two are converging.

THREE QUESTIONS THIS RAISES IN EVERY EXAM

- **Which of our vendors ship AI generated code, and what controls do they attest to?**
  A renewal questionnaire cannot answer this. A daily scan of the code can.
- **Could we detect a malicious or hallucinated package inside a vendor’s product within 24 hours?**
  A live SBOM per vendor answers this with evidence instead of attestation.
- **What is our own shadow AI exposure, and who owns it?**
  If no one owns the answer, the exam finding writes itself.

THE EXAMINER'S PRESSURE STACK

Every framework now expects continuous oversight

Across US and EU supervision, regulators now expect a bank to know what software it runs, where it came from, who maintains it, and how it changes over time. The accountability sits with the bank in every framework.

FRAMEWORK	WHO IT APPLIES TO	WHAT IT NOW EXPECTS
Interagency TPRM Guidance (2023)	Banks supervised by the Fed, OCC, or FDIC	Full lifecycle third party risk management with ongoing monitoring. The bank owns the risk even when the vendor fails.
FFIEC Guidance	Banks, credit unions, and their technology service providers	Third party risk lifecycle, ongoing monitoring, and architectural transparency in vendor relationships, including software components.
NYDFS Part 500	NY licensed institutions and many banks by extension	Third party service provider security policy, asset inventory, vulnerability management, and 72 hour event notification.
GLBA Safeguards Rule	Financial institutions handling consumer data	Written risk assessments, vendor oversight, and continuous monitoring of in scope systems.
SEC Cyber Disclosure	Publicly traded banks and holding companies	Four business day Form 8-K disclosure of material incidents and annual 10-K disclosure of risk management and board oversight.
DORA (EU)	Banks with EU operations and their ICT providers	Register of ICT third party providers, continuous risk monitoring, incident reporting, and resilience testing of critical functions.
SOC 2 / ISO 27001	What banks collect from vendors today	Point in time attestation of controls. Useful as a floor, not a substitute for continuous visibility.

Every framework has moved from periodic check to continuous expectation. A bank that cannot evidence live oversight of its vendor software is not failing a best practice. It is failing the standard its examiners already wrote down.

THE MATURITY CURVE

What good looks like, and what it costs to wait

Most banks sit somewhere on the curve below. The goal of this page is to let an executive team self diagnose in 60 seconds and identify the next stage to reach.

STAGE	HOW IT SHOWS UP	WHAT IT COSTS
STAGE 1 **Checklist**	Annual questionnaires. SOC 2 PDFs in a shared drive. No view inside vendor software.	Exam findings, slow vendor breach response, ad hoc audit scrambles.
STAGE 2 **Periodic**	Tiered annual reviews. Pen test attestations. Contract security clauses. Months long blind spots between cycles.	Late discovery of critical CVEs. Breaches scoped by phone and email. Repeat findings.
STAGE 3 **Continuous**	Continuous visibility into critical vendor software. Live risk scores. CVE alerts routed to owners.	Manual effort to compile exam packets. Limited board visibility.
STAGE 4 **Evidence ready**	Continuous SBOM visibility, vendor risk scores, and CVE posture, with exam ready evidence and board dashboards.	Nothing material. Faster onboarding, stronger exam posture, defensible board narrative.

Most banks we encounter sit at stage 1 or 2. The shift from stage 2 to stage 3 is the single highest leverage move a chief risk officer or CISO can make this year. It changes exam posture, breach response time, and board confidence at once. The cost of waiting is already on the books:

$10.22M
average U.S. breach cost in 2025, an all time high

IBM 2025

267
days to identify and contain a supply chain breach, the longest of any vector

IBM 2025

22%
of breaches began with stolen credentials, often a vendor's

VERIZON DBIR 2025

1 in 6
breaches involved an AI driven attack, averaging $4.49M

IBM 2025

THE DATA BANKS RECEIVE

Live signals across the vendor portfolio

TripleScan runs a daily forensic scan of each critical vendor’s software through a read only repository token. No agents, no pipeline changes, no engineering lift on the bank or the vendor, and vendors participate at no charge.

Tech Risk Score (0 to 100)

A composite score per vendor, updated daily, trended over time, and translated into plain English for board and committee reporting.

Live SBOM per vendor

A full software bill of materials, refreshed daily and queryable across the entire vendor portfolio to surface aggregation exposure in real time.

CVE and license alerts

Severity ranked, mapped to affected vendors and systems, with remediation status and patch latency tracked over time.

Contributor and provenance trail

Who wrote the code, where it came from, and what changed. Critical for incident scoping and post breach root cause work.

FOUR MOMENTS WHERE IT CHANGES THE WORK

- **Vendor onboarding and renewal**
  Replace weeks of questionnaire back and forth with a score derived from the code the vendor actually ships, and tier oversight on observable hygiene.
- **Portfolio aggregation monitoring**
  The same day a critical CVE is disclosed in a widely used dependency, see exactly which vendors and which systems are exposed.
- **Exam and audit evidence**
  Hand examiners live third party software oversight mapped to the Interagency Guidance lifecycle, compiled in hours instead of weeks.
- **Incident response**
  A time stamped SBOM and CVE history already exists for every vendor. Use it to scope exposure before the vendor’s second phone call.

BOARD AGENDA · TEAR OUT PAGE

Ten questions a bank board should ask this quarter

Bring this page to the next risk or audit committee meeting. Ask the chief risk officer, CISO, and CTO to answer each one with evidence, not opinion.

01 **Inventory**
Do we have a live list of every software vendor that touches customer data or money movement, with a current risk posture for each?

02 **Inside the software**
For our ten most critical vendors, can anyone tell us which open source components sit inside their products, and which carry known exploited vulnerabilities?

03 **Concentration**
Which single vendor, if compromised tomorrow, would touch the largest share of our customers, and how would we find out it happened?

04 **The vendor’s vendors**
How far down the chain does our visibility go? The 700Credit breach began at a partner of the vendor, not the vendor itself.

05 **AI exposure**
Which of our vendors ship AI generated code, what controls do they attest to, and what is our own shadow AI exposure?

06 **Known exploited vulnerabilities**
How many CISA KEV catalog entries currently exist across our critical vendor stack, and what remediation timelines do our contracts require?

07 **Incident readiness**
If a vendor notified us of a breach today, how fast could we scope which systems and customers are affected? Can we meet the NYDFS 72 hour and SEC four business day windows?

08 **Exam readiness**
If examiners asked for our third party software risk evidence today, how many person hours would it take to produce, and what would it show?

09 **Board narrative**
Can we hand the board a one page vendor software risk posture today, with trend data, that does not require a technical translation?

10 **Year over year**
Where will we be on the vendor risk maturity curve in twelve months, and what investment does that require?

WHY TRIPLEKEY

Built to put the security boundary outside the system it protects

TripleKey provides real time visibility into software risk and compliance. TripleScan, the company's scan engine, runs daily automated analysis of codebases and dependencies and produces the Tech Risk Score, SBOM, CVE alerts, license conflict detection, and contributor risk analysis. The company was founded in December 2023 and is headquartered in Brentwood, Tennessee. TripleKey monitors software risk in some of the most demanding regulated environments in the country, including enterprise healthcare, where it serves Community Health Network of Indianapolis. TripleKey is not a developer tool and does not touch the bank's or the vendor's pipelines.

GRANTED USPTO INTELLECTUAL PROPERTY

In October 2025, the United States Patent and Trademark Office granted TripleKey US Patent 12,455,973 B1 for a novel approach to secure encryption. The patented system separates cryptographic key custody from the device performing the encryption work, requiring a removable hardware component to be physically present for any decryption to occur. This reflects TripleKey's broader architectural philosophy of moving security controls outside the system being protected, the same philosophy behind TripleScan's out of pipeline monitoring. The patent is wholly assigned to TripleKey and is enforceable through approximately January 2045.

SCALE WITH CONFIDENCE

Let's look at the risk you can actually see.

Bring us your vendor list. We will show you what your critical vendors look like at the code level, and what that means for your next exam, your board narrative, and your customers.

Talk to TripleKey

triplekey.com · Response within 2 business days

TripleKey · 5205 Maryland Way, Suite 300, Brentwood, TN 37027 · triplekey.com

Sources: Verizon Data Breach Investigations Report (DBIR) 2025. IBM Cost of a Data Breach Report 2025 (with Ponemon). National Vulnerability Database, NIST, 2025 to 2026. FIRST 2026 Vulnerability Forecast. CISA Known Exploited Vulnerabilities catalog and emergency alerts, 2025. Identity Theft Resource Center 2025 annual report. Cloud Security Alliance research on Shai-Hulud 2.0, November 2025. USENIX Security 2025 (slopsquatting). Stack Overflow Developer Survey. Deloitte Center for Financial Services. Breach incident details from company notification letters and state regulator filings, as reported by American Banker (December 2025) and PYMNTS (April 2026).