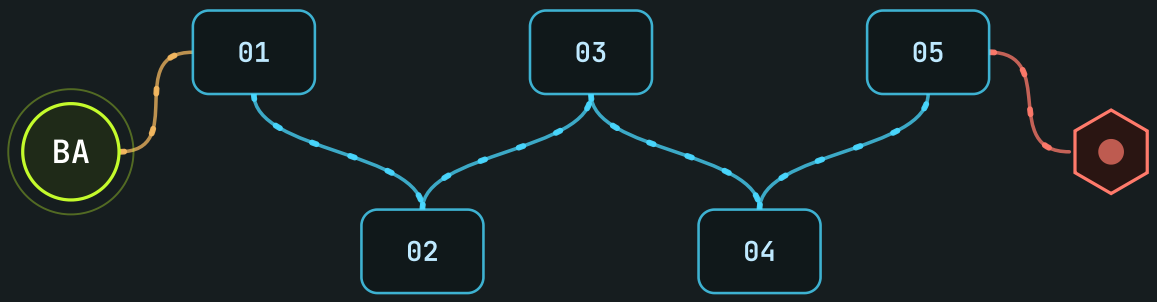


INTELLIGENCE BRIEF

SitusAMC breach moves to a $5.3 million settlement as vendor risk climbs

SitusAMC's 2025 data theft now has a proposed $5.3 million class settlement covering about 662,792 people, and third parties figured in 48 percent of breaches in the 2026 DBIR. Tier vendors by the data they hold.

EDITION
Fall/Winter 2026/2027 Edition
BA-01 · Breach analysis

PUBLISHED BY
Z7 Solutions LLC
Orlando, Florida

READ ONLINE
z7solutions.com
844-974-8669

01 At a glance

STATUS

ONGOING RISK

A final approval hearing on the proposed class settlement is set for November 11, 2026, and no threat actor has been publicly identified in the sources reviewed. [1]

HEADLINE NUMBERS

662,792
People on the settlement class list [2]

$5.3M
Proposed class settlement fund [1]

48%
Breaches involving a third party, 2026 DBIR [12]

16,778
Claims filed as of September 14, 2026 [3]

KEY FACTS

INCIDENT
SitusAMC became aware of unauthorized access on or about November 12, 2025; its letters place the data acquisition between November 12 and November 21 [7]

ATTACK TYPE
Data theft; SitusAMC said no encrypting malware was involved [10]

NOTIFIED INDIVIDUALS
About 662,792 people on the settlement class list [2]

LITIGATION
In re SitusAMC Holdings Corporation Data Breach Litigation, No. 1:25-cv-9748 (S.D.N.Y.) [1]

SETTLEMENT
$5.3 million proposed; claims due November 6, 2026; final approval hearing November 11, 2026 [1]

ATTRIBUTION
None announced in the sources reviewed; the FBI said it was working with affected organizations [10]

02 What happened

SitusAMC, a New York real estate finance services vendor that its website says has more than 1,500 clients, said it became aware of unauthorized access to certain systems on or about November 12, 2025. Its investigation determined that an unauthorized third party acquired data from those systems, including corporate accounting records and legal agreements and, for notified borrowers, names, addresses, dates of birth, Social Security numbers, government identification numbers and financial account information. SitusAMC said no encrypting malware was involved and that its services remained fully operational.

- Press reports citing people briefed on the incident named JPMorgan Chase, Citi and Morgan Stanley among notified clients; SitusAMC did not publicly confirm any client.
- FBI Director Kash Patel told The New York Times the bureau was working with affected organizations and had found no operational impact on banking services.
- FINRA alerted member firms to third-party and fourth-party exposure because banks that use SitusAMC are vendors to broker-dealers.
- SitusAMC mailed notification letters in waves starting January 28, 2026, filed with the California Attorney General on four dates through April 3, 2026, and offered 24 months of IDX identity protection.
- Related federal suits were consolidated in the Southern District of New York, and a $5.3 million class settlement covering about 662,792 people awaits a final approval hearing on November 11, 2026.
- SitusAMC denies wrongdoing, and the court has not decided in favor of any party.

03 How it works

01 Initial access, not disclosed

SitusAMC has not disclosed how the intruder got in. After the incident it said it reset credentials, disabled remote access tools, updated firewall rules and enhanced security settings.

02 Access to internal systems

SitusAMC detected unauthorized access to certain systems in its information technology network on or about November 12, 2025.

03 Data acquired over about nine days

The January 28, 2026 letter states that data was acquired between November 12 and 19, 2025. Letters filed from February 20, 2026 give November 13 to 21, 2025.

04 No encryption, no public ransom note

SitusAMC said no encrypting malware was involved. FINRA described the main goal as large-scale data theft for potential follow-on attacks or extortion, not malware deployment.

05 Downstream fourth-party exposure

FINRA warned that stolen corporate information, accounting records and legal agreements could be used to target broker-dealer customers through those firms' banking vendors that use SitusAMC.

04 Who is at risk

Any organization whose customer data sits with a vendor it does not directly monitor, and any firm whose own vendors use SitusAMC.

- Banks and mortgage lenders that outsource loan fulfillment, due diligence, title, valuation or servicing work
- Broker-dealers and advisers with fourth-party exposure through their banking vendors, as FINRA described
- Pension funds and state governments, which FINRA listed as potentially impacted
- Borrowers whose Social Security numbers, government identification numbers and financial account data were in the acquired files
- SEC covered institutions, which under amended Regulation S-P must notify affected customers as soon as practicable and no later than 30 days after becoming aware of unauthorized access

Sectors in scope: banking and mortgage lending, real estate finance services, broker-dealers with fourth-party exposure, pension funds and state governments.

05 What changed since the last edition

EACH CHANGE WITH ITS SOURCE

01 The court consolidated the related suits into In re SitusAMC Holdings Corporation Data Breach Litigation, No. 1:25-cv-9748, before Judge Lewis J. Liman, with Kelechian v. SitusAMC as the lead case filed November 24, 2025. A July 15, 2026 order records that the court granted consolidation on December 19, 2025 for all but one of eight listed cases; press counts of the consolidated suits vary.

SOURCE 4

02 A $5.3 million class settlement was reported on June 26, 2026. National Mortgage News put the class at about 662,792 people, reported SitusAMC as not admitting wrongdoing or liability, and said a federal judge asked the parties for more information on the settlement administration budget.

SOURCE 2

03 The court-authorized notice went out August 13, 2026. Opt-outs and objections are due October 22, 2026, claims are due November 6, 2026, and the final approval hearing is November 11, 2026 at 10:00 a.m. Benefits are up to $5,000 for documented losses, a flat payment estimated at $75, a $50 California payment and one year of credit monitoring with $1 million of identity theft insurance. The site states that SitusAMC denies doing anything wrong.

SOURCE 1

04 SitusAMC's notification letters filed with the California Attorney General give the acquisition window as November 12 to 19, 2025 in the January 28, 2026 letter and November 13 to 21, 2025 in later letters. The January letter lists name, address, date of birth and Social Security number; the April 3, 2026 letter adds driver's license or other government identifiers and financial account numbers. Both offer 24 months of IDX monitoring.

SOURCE 8

05 Claim uptake is low. Settlement Insight, reporting docket entries, put claims at 16,778 as of September 14, 2026, about 2.6 percent of a 657,845-person class list, with one objection and a fee request of $1,766,666.67 (one third of the fund) filed October 2, 2026.

SOURCE 3

06 Verizon's 2026 Data Breach Investigations Report, as reported by Expert Insights, puts third-party involvement at 48 percent of confirmed breaches, up from 30 percent in the previous edition, across more than 22,000 breaches.

SOURCE 12

07 The SEC's amended Regulation S-P is in force. It requires covered institutions to notify affected customers as soon as practicable and no later than 30 days after becoming aware of unauthorized access, and Sidley reports compliance dates of December 3, 2025 for larger entities and June 3, 2026 for smaller ones.

SOURCE 14

06 What to do now

IN PRIORITY ORDER, HIGHEST IMPACT FIRST

01 DO FIRST **Inventory every vendor and fourth party that holds customer personal data, and tier them by data sensitivity and volume.**

SitusAMC was invisible to most bank customers and to downstream broker-dealers until FINRA named the chain.

02 **Put prompt breach notification, cooperation and audit clauses into every vendor contract that touches customer data.**

SEC covered institutions must notify customers within 30 days of becoming aware, which is unworkable without fast vendor facts.

03 **Require phishing-resistant MFA on every vendor-facing and remote access path and review remote access tooling quarterly.**

SitusAMC said its response included credential resets and disabling remote access tools; check the same paths at your own vendors.

04 **Monitor critical vendors' external security posture continuously instead of relying on an annual questionnaire.**

Black Kite found 129 of 140 financial sector vendors, 92 percent, scored C, D or F for information disclosure in its 2025 report.

05 **Pre-build a vendor breach playbook with regulator and customer notification templates and documented alternate providers.**

The 2026 DBIR counts third parties in 48 percent of breaches, so a vendor incident is now the expected case.

06 **Verify vendor data minimization and segmentation in writing, and ask what customer data they retain after a transaction closes.**

SitusAMC's disclosures describe both corporate relationship files and borrower identifiers acquired in one incident.

07 **Brief leadership on the full cost chain of a vendor breach, not only the settlement fund.**

The $5.3 million fund is one line; 24 months of monitoring, notification, litigation and regulator engagement land on every party in the chain.

08 **Review the identity and Microsoft 365 posture that vendor-facing accounts live in.**

Z7 Solutions™ provides vendor risk assessments and a 24/7 SOC sized for mid-size financial and public sector organizations.

07 Sources

[1] **In re SitusAMC Holdings Corporation Data Breach Litigation, official settlement website** Settlement administrator for the U.S. District Court, S.D.N.Y. · Notice mailed August 13, 2026; accessed October 13, 2026. https://www.samcdatasettlement.com/

[2] **SitusAMC agrees to $5.3 million settlement over data breach** National Mortgage News · June 26, 2026. https://www.nationalmortgagenews.com/news/situsamc-agrees-to-5-3-million-settlement-over-data-breach

[3] **SitusAMC Data Breach Settlement: 16,778 claims by September 14, lawyers ask $1.77 million, objection filed, hearing November 11** Settlement Insight · October 10, 2026. https://settlementinsight.com/news/situsamc-data-breach-settlement-16778-claims-by-september-14-lawyers-ask-1-77-million-objection-filed-hearing-november-11-claim-deadline-november-6-2026

[4] **Stack v. SitusAMC Holdings Corp., order listing cases 25-cv-9748, 9898, 9773, 9824, 9969, 9994, 10043 and 10579 (LJL)** U.S. District Court, S.D.N.Y., via Leagle · July 15, 2026. https://www.leagle.com/decision/infdco20260717757

[5] **Judge consolidates SitusAMC class actions after November data breach** HousingWire · January 16, 2026. https://www.housingwire.com/articles/situsamc-class-action-breach/

[6] **Data breach list entries for SitusAMC Holdings Corporation** California Office of the Attorney General · Entries dated January 28, February 20, March 10 and April 3, 2026. https://oag.ca.gov/privacy/databreach/list?field_sb24_org_name_value=SitusAMC

[7] **Notice of Data Breach letter dated January 28, 2026** SitusAMC Holdings Corporation, filed with the California Attorney General · January 28, 2026. https://oag.ca.gov/system/files/SitusAMC%20-%20Individual%20Notification%20Template.pdf

[8] **Notice of Data Breach letter dated April 3, 2026** SitusAMC Holdings Corporation, filed with the California Attorney General · April 3, 2026. https://oag.ca.gov/system/files/SitusAMC%20-%20Individual%20Notice%20Template.pdf

[9] **FINRA Cybersecurity Alert: SitusAMC Security Incident** FINRA · Undated on the page; the original edition cites December 1, 2025. https://www.finra.org/rules-guidance/guidance/finra-cybersecurity-alert-situsamc-security-incident

[10] **JPMorgan, Citi, Morgan Stanley assess fallout from SitusAMC data breach** CSO Online · November 24, 2025. https://www.csoonline.com/article/4095182/jpmorgan-citi-morgan-stanley-assess-fallout-from-situsamc-data-breach.html

[11] **Intrusion at real estate finance biz sparks concern for big banks** The Register · November 24, 2025. https://www.theregister.com/2025/11/24/situsamc_breach/

[12] **Supply Chain Breaches Surge 60% To Hit Half Of All Incidents (reporting the Verizon 2026 DBIR)** Expert Insights · May 21, 2026. https://expertinsights.com/news/supply-chain-breaches-surge-60-to-hit-half-of-all-incidents

[13] **2025 Financial Services TPRM Report: Vendor Trends** Black Kite · 2025. https://blackkite.com/report/financial-services-tprm-report-2025/vendor-trends

[14] **SEC Adopts Rule Amendments to Regulation S-P to Enhance Protection of Customer Information (Press Release 2024-58)** U.S. Securities and Exchange Commission · May 16, 2024. https://www.sec.gov/newsroom/press-releases/2024-58

[15] **U.S. SEC Regulation S-P: Compliance Deadline Approaching for Smaller Entities** Sidley Austin LLP, Data Matters · April 30, 2026. https://datamatters.sidley.com/2026/04/30/u-s-sec-regulation-s-p-compliance-deadline-approaching-for-smaller-entities/

NEXT STEP

Put the same team on your environment

Talk to the team that runs the Z7 Solutions SOC about what this brief means for your environment. We will tell you what applies and what does not.

ALSO IN THIS EDITION

Qilin still tops most ransomware counts
More from the edition · z7solutions.com/z7-cyber/qilin/

Qilin still hits hospitals and infrastructure
More from the edition · z7solutions.com/z7-cyber/qilin-part-2/

LockBit 5.0 returns after Operation Cronos
More from the edition · z7solutions.com/z7-cyber/lockbit/

CALL 844-974-8669

EMAIL sales@z7solutions.com

BOOK A CALL z7solutions.com/book/

Z7 Solutions™, Z7-Claw™ and Z7-Guard™ are trademarks of Z7 Solutions LLC.