CYBERSECURITYUPDATE

# Black Knight Cyberattack Cripples Mortgage Pipeline as Lenders Scramble

A cyberattack on Black Knight has disrupted mortgage processing for major U.S. lenders, exposing third-party vulnerabilities in a $12 trillion market. Outages halt loans amid rate volatility, prompting regulatory probes and contingency scrambles.

**Black Knight Cyberattack Cripples Mortgage Pipeline as Lenders Scramble**

**Written by Andrew Cain**
Monday, November 24, 2025

In the tightly interconnected world of U.S. mortgage servicing, a cyberattack on Black Knight Inc. has thrown operations into disarray, halting loan processing for some of the nation's largest lenders just as holiday-season refinancing picks up. The incident, confirmed late Saturday, underscores the fragility of third-party tech vendors in financial services, where a single point of failure can cascade across billions in loan volume.

Black Knight, a dominant player in mortgage technology owned by Intercontinental Exchange Inc. (ICE), disclosed the breach on its status page, stating that 'certain services are experiencing an outage due to a cybersecurity incident.' The disruption has idled critical systems for loan origination, servicing, and data analytics, affecting clients like JPMorgan Chase & Co. and Wells Fargo & Co., according to posts found on X from industry watchers and initial reports.

**Vendor Dependencies Exposed in Real Time**



The timing couldn't be worse. With mortgage rates hovering around 6.5% amid Federal Reserve signals of potential cuts, lenders are racing to close deals before year-end. Black Knight's MSP (Mortgage Servicing Platform) and other tools underpin about 60% of the U.S. mortgage market, processing over 12 million loans annually, per company filings. Outages like this echo the 2023 Mr. Cooper breach, which sidelined payments for millions, as reported by The New York Times.

ICE, Black Knight's parent, issued a statement Sunday afternoon: 'We are actively investigating and working to restore services as quickly as possible,' but declined to comment on the nature of the attack or potential data exfiltration. Early assessments from cybersecurity firms point to possible ransomware, though unconfirmed.

**Timeline of the Outage Unfolds**

The incident surfaced around 8 a.m. ET Saturday, with Black Knight's status page flagging 'degraded performance' in its LoanSphere suite, escalating to full outages by midday. By evening, affected services included data delivery, imaging, and flood certification—essentials for underwriting. Lenders reported inability to access borrower credit pulls or generate closing documents, per alerts shared on X by mortgage brokers.

This isn't Black Knight's first brush with cyber woes. In 2021, a ransomware attack on a subsidiary disrupted title services, costing millions in remediation, as detailed in ICE's SEC filings. The current breach adds to a string of 2025 incidents targeting real-estate tech, including SitusAMC's November hack exposing data from JPMorgan, Citi, and Morgan Stanley clients, according to a Reuters report citing The New York Times.

**Cascading Effects on Lenders and Borrowers**

Major lenders have activated contingency plans. Rocket Mortgage LLC, a top originator, tweeted assurances of 'minimal impact' via backup systems, while United Wholesale Mortgage activated manual workflows. Smaller servicers, however, face steeper hurdles, with some delaying closings into December. The Mortgage Bankers Association warned members to 'review vendor SLAs immediately.'

Posts on X from financial pros highlighted escrow risks, drawing parallels to loanDepot's 2024 outage that froze payments, as covered by BleepingComputer. No evidence of data theft has emerged, but Black Knight urged clients to monitor for phishing tied to the incident.

**Regulatory Scrutiny Looms Large**

Federal regulators are circling. The Office of the Comptroller of the Currency (OCC) and Federal Housing Finance Agency (FHFA) have requested briefings, sources familiar with the matter said. This follows CSIS's timeline of significant cyber incidents, which logs over 50 major attacks on financial firms since 2020, including state-sponsored espionage.

Black Knight's role as 'mission-critical' infrastructure—certified under NYDFS cybersecurity regs—amplifies the stakes. A prolonged outage could spike delinquency rates if payments glitch, mirroring Mr. Cooper's 2023 fallout where four million customers faced delays, per BleepingComputer.

**Industry's Third-Party Risk Reckoning**

For insiders, this is a wake-up on vendor concentration. Black Knight commands 65% market share in servicing platforms, per insider estimates, leaving little room for diversification. Firms like ICE have invested in zero-trust architectures post-2021, but experts say multi-factor authentication and air-gapped backups remain uneven.

Cybersecurity analysts at The Hacker News noted similar tactics in recent attacks, with nation-state actors like those behind Black Hat 2025 demos targeting supply chains. 'This is the plumbing of housing finance,' tweeted one X user from a distressed-debt fund, echoing broader credit-system fears.

**Path to Restoration and Resilience**

As of Monday morning, partial services flickered back online, with full restoration eyed for mid-week. ICE shares dipped 1.2% in premarket trading, reflecting investor jitters over liability. Lenders are now stress-testing alternatives like Enact MI or CoreLogic, though switching costs run into millions.

The breach spotlights 2025's cyber escalation: CSIS reports a 30% uptick in financial attacks, fueled by AI-driven phishing. For mortgage execs, the mandate is clear—deeper vendor audits, contractual kill-switches, and cyber insurance riders tuned for systemic risks.





**Notice an error?**

Help us improve our content by reporting any issues you find.

Request Correction