Challenge Prompt – Loan Depot

Cybersecurity Breach Event Scenario & Response

Prepared by: Aydan Paul, Emma Lewis, TJ Fields, and Toshan Misir

November 4, 2025

Scenario

It was the first week of January 2024. Loan Depot staff were returning from their holiday breaks, easing their way back into work for a new year. On January 4th, the network operations center was running their normal morning checks. Everything looked routine at first, until a systems engineer noticed something off: there were unexplained error messages in the company's loan servicing logs. These messages indicated timeouts and failed database connections that did not match any maintenance schedules.

Minutes later, as employees started to hurry inside from the frigid winter temperatures to their desks, they started reporting trouble accessing internal applications. The helpdesk was receiving calls from customers indicating that they had strange file names and unfamiliar extensions in their accounts, with one caller stating there was a pop up on her screen stating, "*Your files have been encrypted.*"

By midmorning, the issue became clear- there was a breach in the system. Core servers tied to loan origination and customer service were locked and attempts to restore the backups had failed. Suddenly, a ransom note appeared on many workstation computers-

"*We have access to sensitive data pertaining to 17 million people. We demand money, and if we do not receive that money, we will release this data.*"

Customers continued flooding the help desk support lines, unable to access their accounts or make mortgage payments. Within hours, the company reported the incident to authorities and began notifying regulators and cybersecurity partners of the breach. Who was behind this breach, and how would we recover the data?

Background

Loan Depot was founded in 2010 by Anthony Hsieh, who worked in the mortgage industry. The company was headquartered in Irvine, California, and licensed in every state, with branches across the US. From the beginning, Loan Depot has focused on retail mortgage

lending and serving as a "non-bank" lender. They promote an effortless and straightforward mortgage experience, where customers are their sole priority.

Loan Depot has consistently maintained a digital-first approach when it comes to financing and lending to its customers. They integrate their use of the Mello software platform to enable direct-to-customer channel sales. This strategy allows the company to generate revenue through its home loans, servicing charges, and home equity products. At the end of 2023, Loan Depot reported revenue of $974 million, which was down from 2022. By quarter 2 of 2024, Loan Depot had seen significant improvements in its productivity cost, as evidenced by its reported revenue of $265 million.

Although Loan Depot saw significant improvements in its productivity costs between January 3rd and January 5th, the company faced a significant security breach in which an unauthorized third party accessed some of its systems, affecting approximately 17 million individuals. The company reported that data, including names, addresses, emails, phone numbers, social security numbers, financial account information, and dates of birth, were all compromised.

Loan Depots' first response was to take all systems offline to help contain and prevent further growth of the breach. After those systems were shut down, their forensic investigators went in to investigate the incident, discovering just who was impacted and what data was compromised. They also investigated how these attackers gained access to the information. After notifying every compromised individual, they offer services free of charge and new protection amenities.

Loan Depot faced legal repercussions and ultimately settled for $25 million among all individuals involved. Due to Loan Depot including the cost of enhancing their security, investigating, and additional monitoring, their incurred costs far exceeded their payout. They not only incurred financial losses but also suffered a reputational breach, which affected Loan Depots' reputation and led to a loss of trust from customers and stakeholders.

They are not yet fully profitable or thriving, but they continue to show steady improvement. The company is gradually rebuilding customer trust while managing ongoing cost challenges.

Breach

In early January 2024, Loan Depot experienced a ransomware and data theft attack. The company discovered unauthorized access to its network and responded by shutting down several internal systems to contain the intrusion. The APLHV/BlackCat ransomware group later claimed responsibility for the attack.

During the breach, attackers accessed and exfiltrated sensitive personal information (SPII) belonging to about 16.6 to 16.9 million customers. The compromise data included addresses, names, D.O.B, SSN, and in some cases financial account numbers. The attackers also encrypted data and systems, disrupting operations and temporarily preventing some customers from accessing online accounts and loan services.

Loan Depot notified federal and state regulators, filed SEC disclosure, and began notifying impacted individuals. The company offered affected customers' identity theft monitoring and credit protection services. In addition to customer impact, the incident resulted in operational disruptions, reputational damage, and millions of dollars in incident response and recovery costs.

The exact initial cause of the breach has not been publicly conformed, but the attack followed patterns commonly associated with the BlackCat ransomware group, which often uses credential compromise, phishing, or exploitation or remote access systems to gain entry.

Case Questions

1. What were the biggest mistakes LoanDepot made before, during, and after the breach?
2. How should LoanDepot rebuild customer trust post-incident?
3. How can they improve backup integrity and isolation?
4. What governance failures contributed to the incident (e.g., lack of oversight, funding, KPIs)?
5. What role should the CISO, CEO, Board, and Legal Counsel play during the first 24 hours?
6. How should LoanDepot evaluate the effectiveness of its incident response after the event?
7. What regulatory reporting requirements apply (FTC Safeguards Rule, GLBA, SEC Breach Disclosure, State AG laws)?
8. Did Loan Depot's *Respond* actions align with NIST 2.0 best practices? Why or why not?

9. What *Recover* activities should LoanDepot prioritize to restore operations and rebuild trust?
10. Why did backups fail, was it encryption, corruption, or lack of network segmentation?

Sources

Aijaz, Duresham. “Loandepot Data Breach Wasn’t Just a Glitch - Find out More.” *PureWL*, 7 May 2025, www.purewl.com/loandepot-data-breach/.

“Corporate Overview.” *loanDepot Inc. - Investor Relations*, investors.loandepot.com/overview/default.aspx. Accessed 6 Nov. 2025.

News Releases | Loandepot, Inc.., media.loandepot.com/news-releases/. Accessed 6 Nov. 2025.

Team, StrongDM. “Loandepot Data Breach: What Happened and How They Solved It.” *StrongDM*, StrongDM, Inc., 16 Apr. 2025, www.strongdm.com/what-is/loandepot-data-breach.

Top Class Actions. “$25M Loandepot Data Breach Class Action Settlement.” *Top Class Actions*, 7 Mar. 2025, topclassactions.com/lawsuit-settlements/closed-settlements/25m-loandepot-data-breach-class-action-settlement/.