



CUSTOMER STORY

How a Fortune 500 financial institution uses behavioral data to prioritize digital investments



CHALLENGE

Users were abandoning the online banking enrollment process at an alarming rate, citing difficulties during the security question setup and VeriD verification phases.

Pre-Fullstory, a \$1M investment was earmarked to overhaul their loan conversion module, but the lack of user behavior data and module performance posed a significant risk, causing concerns about opportunity costs and ROI.

Amidst receiving numerous support cases raising concerns of fraudulent activities, the organization struggled to conclusively validate these claims, resulting in operational inefficiencies, customer frustration, and financial risk.

The password change conversion rate had been steadily declining, dropping to a low of 33.2%. This suggested users were encountering barriers while trying to update their passwords, but the exact reasons were unclear.

SOLUTION**Indexed Autocapture**

Armed with Fullstory's ability to automatically capture events (no tagging or instrumentation required) and use session replay to understand the issue, the Product team immediately diagnosed the problem and confidently took action to implement a fix.

Robust Analytics

Leveraging Fullstory's robust analytics capabilities — dashboards and metrics tuned to provide granular insights into user engagement levels, traffic distribution among various modules within their B2B banking platform, etc., — the organization realized they needed to pivot.

Session Replay + UUIDs

Through leveraging Fullstory's session replay functionality — and coupled with specific user IDs — the organization gained immediate access to specific, detailed session replays that provided irrefutable evidence of fraudulent activities within their digital banking environment.

Segmentation + Session Replay

By segmenting users who were unsuccessful in changing their passwords, the team analyzed sessions to uncover the underlying issues. The password requirements—like character length, special characters, etc.—weren't clear. This lack of transparency led to user frustration and failed attempts at changing passwords.

OUTCOME**+10.8%**

in the enrollment conversion rate (from 18.5% to 29.3%) within five days, post-launch.

\$1,000,000

Poor ROI project avoided. More notably, a paradigm shift in their decision-making framework that now drives all digital investments.

Lower risk

A step change in the fraud resolution process significantly improved the organization's ability to protect its customers and mitigate financial risk.

+51.7%

in the conversion rate for password changes (now 84.9%) after revising and clearly displaying the password requirements.