

Customer Case Studies

CASE 1: LARGE MEDICAL COMPANY ENHANCES SECURITY WITH ASSET MANAGEMENT TAGS

A large US Fortune 500 medical company required a secure user verification process at the help desk after detecting attempts by unauthorized individuals to gather sensitive information. To address this, they implemented FastPass with a combination of data from their HR system, presenting only partial elements of correct answers to the support team.

A key component of their strategy involves asking users to provide the asset number of their PC or using their phone for additional verification. For users in privileged groups, a stricter verification process is triggered, and cases are often escalated automatically to a higher level, still managed by FastPass. The company has integrated [FastPass on-premises with their existing ServiceNow platform](#).



CASE 2: FINANCIAL ORGANIZATION INTEGRATES FASTPASS AND OKTA FOR ENHANCED HELP

A smaller US financial organization with 3,000 users had already invested in OKTA for multi-factor authentication (MFA) and wanted to strengthen their defenses against social engineering attacks. After learning about a security breach at another financial institution, they sought a simple yet robust verification process.

With FastPass, [the help desk sends an OKTA push notification to users needing verification](#), protecting not only password-related inquiries but also other call types. The organization uses [FastPass Cloud integrated with ServiceNow for comprehensive security](#).

CONTACT US:

UK : + 0333 3200513
Europe : + 45 4810 0410

 info@fastpasscorp.com
 www.fastpasscorp.com

CASE 3: UNIVERSITY IMPLEMENTS SECURE VERIFICATION FOR STUDENTS AND STAFF



A European university faced incidents of students attempting to access others' accounts by requesting password resets from the help desk. Concerned about the potential for unauthorized access to central data resources containing student and alumni information, they turned to FastPass for a solution.

The university opted to use SMS as part of the verification process, leveraging their existing database of student phone numbers. If a student couldn't access their phone, a set of security questions was used instead. Staff and faculty were required to connect their MS Authenticator to FastPass for secure verification. To further reduce the help desk workload, [FastPass's self-service password reset](#) feature was also implemented.

The university integrated [FastPass on-premises with their local ITSM system](#).

CASE 4: SERVICE PROVIDER (MSP) ENHANCES SECURITY AND COMPLIANCE WITH FASTPASS

An international service provider managing IT help desks for numerous clients faced growing demands for secure user validation when handling service requests and password resets. Both their customers and the service provider's management were increasingly concerned about the potential consequences of a data breach caused by inadequate verification at their help desk.

By implementing [FastPass Identity Verification Manager \(IVM\)](#), the service provider found a solution that seamlessly integrates with their ITSM system, allowing them to manage multiple client accounts without needing to switch between different systems. This streamlined workflow ensures consistent and secure service, regardless of which customer contacts their service desk.

Additionally, the service provider can now provide real-time compliance reporting to clients, complete with a detailed log of all verification activities and documentation confirming the secure delivery of new passwords. Importantly, this move to a more secure validation process has been achieved without any negative impact on productivity.

CONTACT US:

📞 UK : + 0333 3200513
Europe : + 45 4810 0410

✉️ info@fastpasscorp.com
🌐 www.fastpasscorp.com

 **FASTPASSCORP**