yubico

YubiKey for Financial Services Call Centers

61% of fraud traced back to contact center

Fraud loss will double from $393M in 2015 to $775M in 2020

Aite Group 2019

Based on interviews of 25 executives at 18 of the top 40 largest U.S. financial institutions

www.pindrop.com/blog/61-of-fraud-traced-back-to-the-contact-center/

Three ways financial services call centers can increase authentication security and user experience

Financial services call centers or the contact centers manage large daily call volumes and call center agents need fast, secure and regulation-compliant access to important customer, account and financial data, to quickly maximize customer satisfaction and achieve key call center success metrics. But currently used authentication methods including mobile phone-based authentication don't offer highest-assurance security against call center fraud and account takeovers.

In 2019, Aite Group interviewed 25 executives at 18 of the top 40 largest U.S. financial institutions, and found that 61% of fraud can be traced back to the contact center. They predict that contact center fraud loss will double from $393 million in 2015, to $775 million in 2020. With high employee churn, seasonal peaks, and other challenging business dynamics, call center environments need a secure, yet simple approach to verify agent identities before providing access to critical systems and data.

Below are three ways financial services call centers can increase authentication security and user experience:

Maximize call center productivity with security keys

Personal mobile devices in call centers impact performance

Many employees use their personal devices to make phone calls, send texts, or check their social media accounts while they're on the clock. In order to maximize productivity, the use of personal mobile devices should only be allowed off the call center floor. Using personal mobile devices for mobile phone-based authentication impacts performance and lowers call center metrics such as minimal customer time in call queue; first contact resolution; and average handling time.

Financial services call centers can enable strong authentication for agents without having to use mobile phones. Unlike SMS codes and mobile push authentication, hardware security keys such as the YubiKey do not require a cellular connection, batteries, or any other external dependency to operate. Call center agents can simply plug a security key into a USB port on a computer or other system and touch to authenticate.

Mitigate against insider threat risks with mobile-restricted authentication

Mobile device authentication puts sensitive customer and financial data at risk

Call center agents are trusted with access to highly sensitive customer and financial data. With such sensitive and protected data at stake, personal mobile devices and their cameras introduce unnecessary risk of sensitive data leakage. The 2019 Verizon Data Breach Investigations Report found that Privileged Misuse was among the top 3 breach patterns for the Financial and Insurance Industry. Using mobile devices for 2FA allows call center employees to easily capture sensitive data on camera without being noticed, putting the organization at great risk.

Hardware security keys can deliver stronger security to protect customer account information, offering more peace of mind than SMS-based authentication or mobile push. By eliminating the dependence on mobile phones, call centers can ensure that agents cannot capture images of customer and financial data such as account numbers, card expiration dates, and numerous other details that might violate customer privacy.

Meet stringent compliance requirements with highest levels of assurance

Mobile devices don't meet stringent compliance requirements to protect data and privacy

The importance of compliance in financial services call centers cannot be overstated. Call centers usually rely on PII to verify a caller's credentials, and need to ensure information such as social security numbers, bank card numbers, date of birth, or email addresses is protected. Therefore it is imperative that strong authentication is enabled for call center agents to abide by relevant regulations such as SOX, PCI, GDPR, FIPS and PSD2 during every instance of customer engagement.

By implementing hardware security keys, call centers can effectively protect sensitive data and consumer privacy. Call centers should put a strong authentication solution in place that can securely verify the identity of call center agents before they are given access to PII and other sensitive data, or make any changes to a customer account, such as raising a credit limit.

Prevent call center fraud and achieve highest-assurance authentication security with the YubiKey

Hardware security keys such as the YubiKey, offer a modern, highly secure, easy to use, and cost-effective alternative to using mobile phones as a 2FA mechanism, by storing a user's credential securely on the hardware form factor which cannot be exfiltrated. In addition, by eliminating the dependence on mobile phones, call centers can ensure that agents cannot capture images of customer and financial data that might violate customer privacy.

The YubiKey is a multi-protocol hardware security key that enables strong MFA of call center agents before providing access to sensitive and PII data, keeping financial services organizations compliant with existing and emerging regulations including SOX, PSD2, PCI, FIPS, and GDPR. Unlike SMS codes and mobile push authentication, YubiKeys do not require a cellular connection, batteries, or any other external dependency to operate- instead, call center agents can simply plug the YubiKey into a USB port on a computer or other system and touch to authenticate.

Learn more about the *Essentials for Enabling Strong Authentication in Financial Services Call Center* here.

Yubico AB
Kungsgatan 44
2nd floor
SE-111 35 Stockholm
Sweden

Yubico Inc.
530 Lytton Avenue, Suite 301
Palo Alto, CA 94301 USA
844-205-6787 (toll free)
650-285-0088