yubico

APRIL 2020

Essentials for Enabling Strong Authentication in Financial Services Call Centers

Secure access to data. Trusted customer service.

Introduction

In the financial services industry, the call center or the contact center environment is fast-paced, managing large transaction volumes on a daily basis. They typically operate 24/7, with customer service agents logging in and out of key systems, across multiple shifts. The financial services industry is also highly regulated and call centers need to prove compliance to SOX, PSD2, PCI, FIPS, GDPR and other industry mandates.

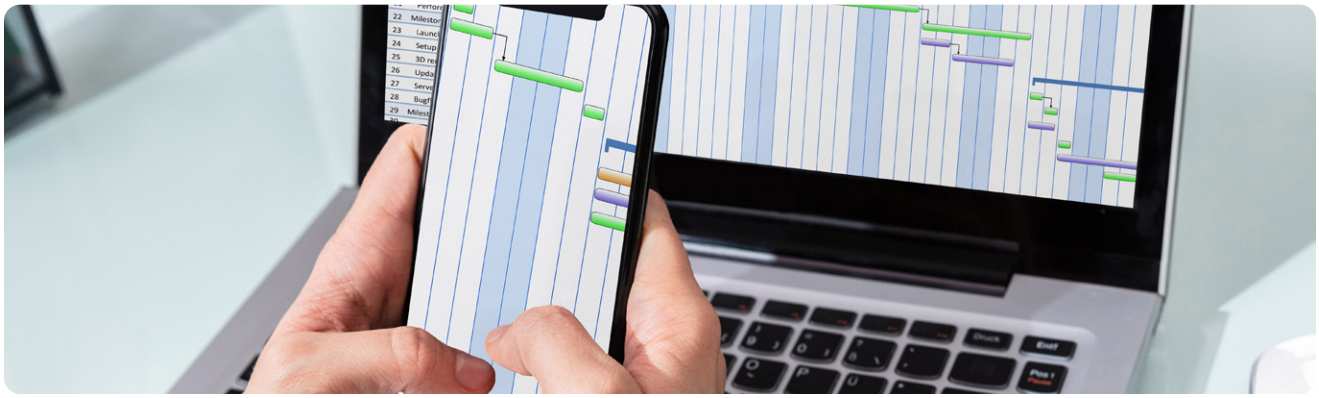
Call center or contact center agents need fast, secure and regulation-compliant access to important customer, account and financial data so that they can quickly maximize customer satisfaction and also achieve key call center success metrics including, minimal customer time in call queue; first contact resolution; and average handle time. With high employee churn, seasonal peaks, and other challenging business dynamics, the impetus to get call center employees productive quickly, and ensure security controls are in place, is of utmost importance. 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.[1]

Call center environments can greatly benefit from a secure, yet simple approach to verify the identity of their agents before providing access to critical systems and data so they can quickly provide excellent customer service.

[1] https://www.pindrop.com/blog/61-of-fraud-traced-back-to-the-contact-center/

Mobile phone-based authentication creates risks

Given the sensitive PII, account information and financial data accessible to customer service agents, properly protecting that data is critical. Anyone accessing sensitive information is typically required to follow regulatory requirements for strong authentication, including two-factor authentication (2FA). However, many two-factor authentication offerings require the use of a mobile phone. The use of mobile phones within call centers poses particular challenges due to security, productivity, and compliance risks.



Personal 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.

Insider threats from call center workers with access to sensitive information

Call center agents are trusted with access to highly sensitive customer and financial data. With such sensitive and protected data at stake, it is critical that personal mobile devices are not used to capture images and sold to malicious actors. 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 enables call center employees to easily capture sensitive data on camera without being noticed, putting the organization at great risk.

Stringent compliance requirements to protect data and privacy

The importance of compliance in financial services call centers cannot be overstated. Compliance is a factor for organizations in almost every sector whenever sensitive data is being stored or accessed. Call centers usually rely on PII to verify a caller's credentials and need to ensure information such as social secuity numbers, bank card numbers, date of birth, or email addresses is protected. Therefore it is critical to ensure 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.

Two-factor authentication using mobile devices exposes call centers to numerous risks. Recent breaches have also proven that the use of SMS, mobile push, and related mechanisms leave organizations and its users highly vulnerable to data theft. As call centers are crucial to customer satisfaction and the viability of an organization, it is critical that strong authentication is enabled to protect valuable data.

Benefits of strong authentication with security keys

Hardware security keys offer a modern, effective, 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. Hardware security keys are ideal for mobile-restricted environments such as call centers. A multi-protocol hardware security key that leverages many different authentication protocols on a single device can easily provide the flexibility that call centers need.

Key benefits of a hardware security key implementation:

Maximize call center productivity

Call centers can enable strong authentication for agents without mobile phones that can be distracting and hamper productivity. Unlike SMS codes and mobile push authentication, hardware security keys do not require a cellular connection, batteries, or any other external dependency to operate. Users 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

Hardware security keys can deliver stronger security to protect customer accounts, 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 details that might violate customer privacy.

Meet stringent compliance requirements

By implementing hardware security keys, call centers can effectively protect sensitive data and consumer privacy. Call centers can 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.

Call center authentication use cases

A hardware security key, such as the multi-protocol YubiKey, enables call centers to support a variety of authentication use cases. The YubiKey also integrates with the majority of Identity and Access Management (IAM) and Single Sign-On (SSO) solutions.

YubiKey smart card deployment for workstation login

Many call centers leverage virtual desktop infrastructure (VDI) to improve security and operational efficiencies. The YubiKey works with VDI software to provide a seamless and secure login experience. For a more efficient initial login to the call center, the YubiKey can be deployed as a smart card to replace the login password. Instead of entering a password to login, a call center agent simply presents their YubiKey (USB or NFC may be used) and enters a PIN that changes rarely, if ever.

There are numerous benefits for implementing YubiKey as smart cards for initial login, including:

Faster login/logout experience

Using YubiKeys as smart cards eliminates the need for users to enter usernames and passwords to authenticate. Agents can use easy to remember PINs that are not stored on a server and do not expire. If a YubiKey is unplugged, a lockout or logout event can be triggered to provide an added layer of security.

Fewer IT service desk calls

Leveraging the YubiKey to log into a workstation with a PIN reduces the number of passwords call center agents have to remember and therefore the number of calls to the service desk when passwords are forgotten.

Built-in 2FA

Smart card implementations meet 2FA requirements. In addition, most federation tools have built-in smart card support to enable single sign-on and/or 2FA support.

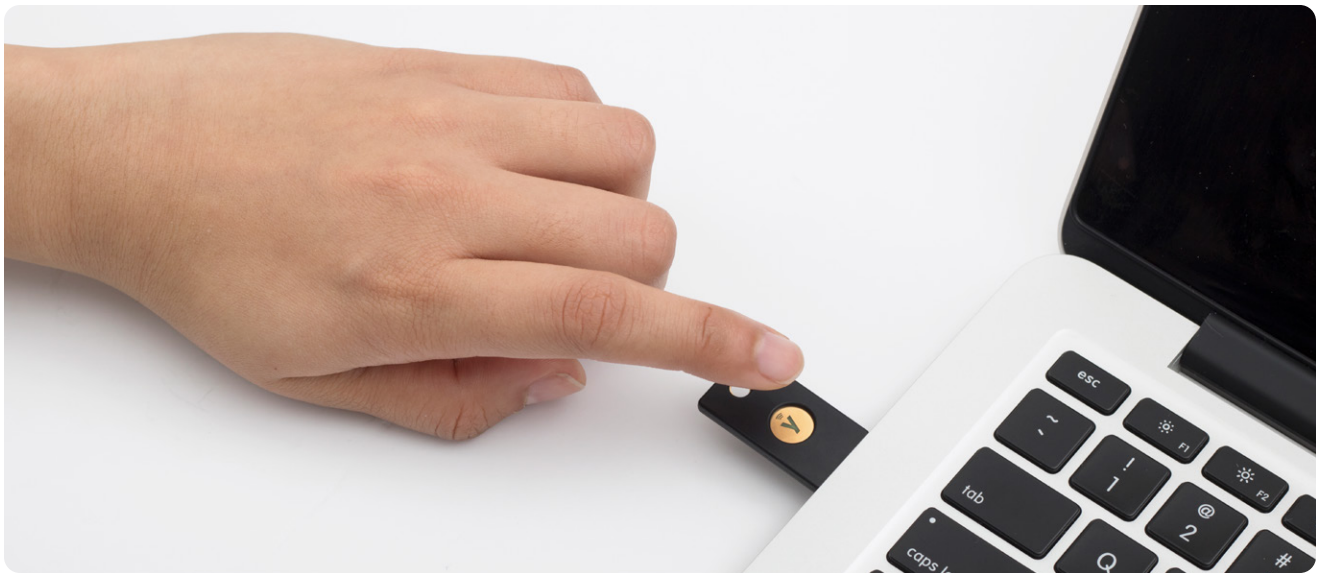
Strong authentication with granular controls

YubiKeys meet the highest authentication standards such as NIST SP 800-63. Additionally, in a Microsoft environment, the system can recognize whether an operator logs in with a smart card or with a username and password. This enables additional access to be automatically granted when the system recognizes a user logging in with a smart card.

Locally managed onboarding tools

Out-of-the-box and third party tools can be used to delegate the management of smart cards to front-line personnel. Call centers have flexibility in how they manage onboarding, support, and offboarding events. Tools are also available to provide self-service, local management, or centralized support to manage smart cards.

The capabilities of the YubiKey greatly streamline smart card deployment in organizations. However, implementing the YubiKey as a smart card does require a PKI environment, which can be anywhere from straightforward to complex, and care should be taken to design the environment for the call center's specific needs.



Strong 2FA options with the YubiKey

The YubiKey is commonly used to provide a second factor for authentication, as a layer of protection above and beyond usernames and passwords. This provides additional security and meets a number of regulatory and customer requirements that call centers must adopt. With YubiOTP (OTP = one-time passcode), the YubiKey provides commonly used OTP-based capabilities as well as more enhanced OTP capabilities.

The YubiKey also supports the FIDO2 and U2F modern authentication open standards, which Yubico pioneered, working with the FIDO Alliance. These standards combine high security with ease-of-use to provide additional protection against phishing attacks. YubiKeys also support standard time based (TOTP) and hash based (HOTP) one-time passcodes that are common across the industry. The YubiKey is not bound to a mobile device, making it an ideal option for call centers nor does it require a PKI environment.

The YubiKey offers several benefits as a 2FA solution:

Strong security

By leveraging the modern authentication protocols, the hardware security key provides very strong second-factor authentication. Additionally, YubiKeys provide a strong and flexible OTP solution.

Ease of use

Less time is wasted logging into systems with the YubiKey. By requiring a user to do no more than touch the YubiKey instead of requesting, receiving, and typing in a code, 2FA significantly speeds up the user login process. Google did an extensive study and found that using YubiKeys decreased login time by nearly 50 percent. In a call center where time is critical, this increase in operational efficiency is significant. The more applications an agent needs to log into, the more important this becomes.

Durability

YubiKeys are extremely durable. The keys do not require cellular or internet access to function properly so they can be used in any environment. Additionally, unlike phones or apps, they do not need to be updated or charged.

High ROI

2FA setup can be done via self service and does not require an IT administrator. Deployment of keys to new call center employees is very quick and cost-effective.

Best Practices for deploying and managing the YubiKey in a call center

To maximize success, ensure strong security, and deliver ROI, there are recommended best practices for YubiKey deployment in a decentralized hardware-based authentication mode.

As call center operations vary by organization, a key factor in the deployment and management of hardware security keys is to determine the requirements and operational environment of the call center. The management of YubiKeys should align with other operational controls, including processes to report and revoke access for lost keys.

Strict security controls

Strict controls of YubiKeys can be addressed by distributing keys at the beginning of a shift and having keys returned to the manager or security guard at the end of the shift. In this scenario, the keys never leave the building and are secured while not in legitimate use. This procedure can be adopted for reasons of economy as well. To ensure the keys are returned, some companies have check-in and check-out processes where employees exchange personal belongings, such as their mobile phone with YubiKeys. When the call center employees return the YubiKeys, their phone or other personal belongings are returned. For easier identification, YubiKeys can be attached to a lanyard along with the company badge.

Medium security controls

If strict controls are not required, an employee would have control of the key but would only be issued one YubiKey. If the employee loses the key, they would need manager approval to receive another YubiKey from the security team. Alternatively, a simple notification could be sent to the manager when a YubiKey is issued. The security team would also deactivate the lost YubiKey. This reduces friction for the employee and allows the manager to only take action when needed. All employees would be required to return their YubiKeys upon leaving the organization.

Low security controls

At a low level of control, employees have control of their YubiKeys at all times and do not need to return them at the end of their shifts. If an employee loses or forgets their YubiKey, a self-service process could be used to ensure the employee can quickly return to work. Some companies have installed vending machines that dispense YubiKeys so an employee can quickly acquire a new key. The employee could be required to pay for the replacement YubiKey.

For virtual call centers, it is recommended that the employee have a backup YubiKey that can be used if the primary key is lost. In this use case, it is assumed that employees are not required to return YubiKeys as workplace efficiencies are more important.

Following a recommended approach in deploying and managing YubiKeys ensures fast and effective user adoption and maximum security for critical assets. With specific security requirements and high turnover in call centers, it is important to note that YubiKeys do not pose a security risk if they are lost, stolen, or not returned when employees leave an organization. YubiKeys can be retained or reset for reuse, based on needs and requirements. More information on reusing YubiKeys, an be found at YubiKey LifeCycle Management - Key Retirement.

Summary

Hardware security keys, such as the YubiKey, offer strong security while keeping the user experience fast, easy, and convenient. With no dependence on cell connectivity, mobile phones, or other tools that can pose both security and productivity risks, security keys are an ideally suited strong authentication solution for call centers. The YubiKey provides an array of authentication options to address common call center use cases and ensures operational efficiency, while keeping security levels high and delivering strong security ROI.

yubico

About Yubico

Yubico sets new global standards for simple and secure access to computers, mobile devices, servers, and internet accounts.

The company's core invention, the YubiKey, delivers strong hardware protection, with a simple touch, across any number of IT systems and online services. The YubiHSM, Yubico's ultra-portable hardware security module, protects sensitive data stored in servers.

Yubico is a leading contributor to the FIDO2, WebAuthn, and FIDO Universal 2nd Factor open authentication standards, and the company's technology is deployed and loved by 9 of the top 10 internet brands and by millions of users in 160 countries.

Founded in 2007, Yubico is privately held, with offices in Sweden, UK, Germany, USA, Australia, and Singapore. For more information: www.yubico.com.

© 2020 Yubico