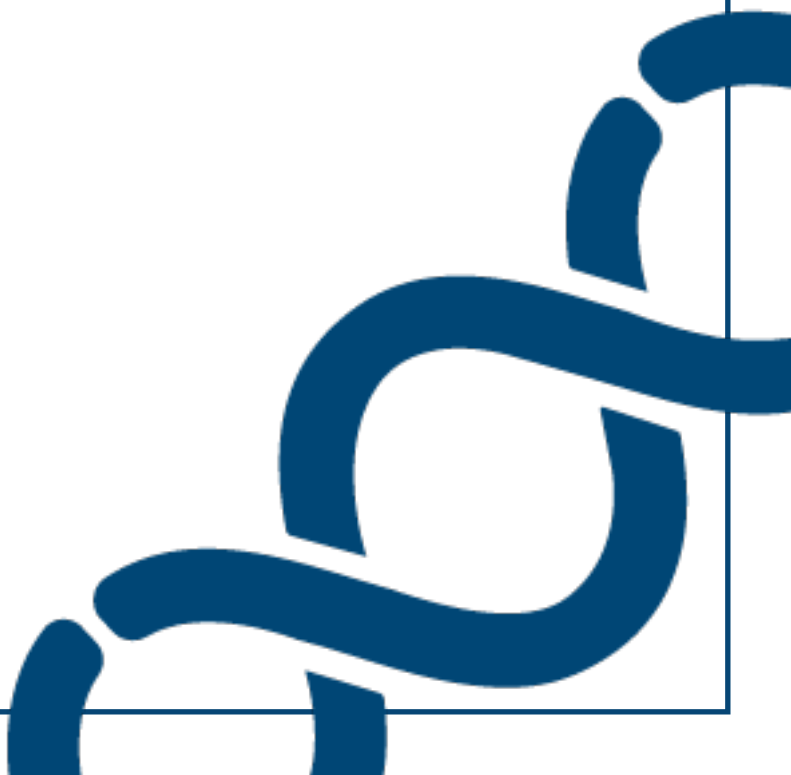
TWOSENSE

# Becoming PCI DSS 4.0 Compliant with Behavioral Biometrics

A Whitepaper



## Introduction

Contact centers are  stuck between a rock and a hard place: PCI DSS compliance and the available technology. Meeting the required standards is difficult when the current MFA solutions available simply do not meet requirements.

To further complicate the situation, the new PCI 4.0 standards that will take effect in March 2024 have been published, and they are even stricter than PCI 3.2.1. With only 21 months remaining to implement updated security policies and procedures, it is critical that organizations review the section 8 requirements and develop a plan to meet them.

Cutting corners on compliance is not an option; the security requirements mandated by PCI and NIST are critical when it comes to securing cardholder data environments. BPO contact centers have been the targets of multiple high-profile breaches in 2022, and are likely to continue as attackers realize that BPOs have access to their customers' networks.

As hackers' technologies and strategies become more sophisticated, the PCI authentication requirements have evolved to meet them.  Thus, maintaining best practices and utilizing the tools and guidance provided by the PCI SSC is critical both for compliance and an effective security posture.

In this whitepaper we will discuss common PCI compliance mistakes and recommendations on how to solve them, walk through the upcoming changes to PCI DSS 4.0, and discuss why behavioral biometric multi-factor authentication is the only available solution to meeting and maintaining compliance for contact centers.

# TABLE OF CONTENTS

## Section 1: Surviving a PCI Audit

### PCI and MFA- A Brief History

In April 2016, The Payment Card Industry Security Standards Council (PCI SSC) published PCI DSS version 3.2. These Data Security Standards were developed to encourage and enhance cardholder data security and facilitate the broad adoption of consistent data security measures globally. One of the most significant additions to PCI DSS 3.2 was that starting February 1st, 2018, **multi-factor authentication** became mandatory per requirement 8.3.1 of Identify and authenticate access to system components.

The addition of MFA in the 3.2 requirements was a significant step towards making credit card transactions and the organizations processing them more secure, as the previous version 3.1 only required two-factor authentication.

In November 2018, the PCI SSC published Protecting Telephone-Based Payment Card Data 3.0. This particular document provided further clarity on guidance for telephone-payment environments to better manage the risk of fraudulent activity. One recommendation which is widely adopted by contact centers is Section 4.1- Risks and Guidance in Simple Telephone Environments, which encourages facilities that process payment transactions to implement physical controls such as restricting mobile phones at agents' workstations or on the contact center floor.

"Restricting the recording of account data is essential to maintain a secure environment. This may mean implementing processes to restrict access to: notebooks and pens, mobile phones capable of taking notes, any device that enables voice recordings, and where account data is input into a system any device capable of taking pictures."

These restrictions made passing a PCI audit incredibly difficult for BPO contact centers.

## The Cost of Non-compliance

Non-compliance comes with some pretty serious repercussions. Loss of the ability to accept credit cards is the most terrifying risk that organizations take if they are not diligent about maintaining compliance. The inability to process credit card transactions would be detrimental to most organizations, and would be a situation many would not survive.

When it comes to an organization's brand, failing to maintain compliance could cause significant harm to their reputation. Reputational damages can seriously impact an organization's ability to acquire new clients and their ability to retain current clients.

The final risk would come in the form of fines. Non-compliance fines can range anywhere from $5,000 to $100,000 per month until compliance is obtained. These fines do not include the cost of remediation, any potential infrastructure updates that might be necessary, or the cost of having a Qualified Security Auditor (QSA) evaluate your current infrastructure, which can often cost upwards of $100,000 alone.

Ultimately, when it comes down to maintaining PCI DSS compliance, being proactive is a must. There is a surplus of vendors providing services that run the gamut when it comes to consulting and solutions. Finding a partner that is able to address your particular needs and supplement experience where teams may be limited is one of the best approaches to ensure company systems, policing, and procedures are up to standards.

## Common MFA Mistakes

The most common mistake with MFA is misunderstanding what is meant by "multi-factor authentication." MFA is defined by NIST as "An authentication system that requires more than one distinct authentication factor for successful authentication. The three authentication factors are something you know, something you have, and something you are (e.g., biometric)." Some BPO call centers implement two different passwords, or a password and a knowledge-based-authentication question like "what

was your childhood pet?" While these are technically multiple factors, the fact that both are "something you know" means that they don't qualify as true MFA.

Similarly, some organizations set up multiple factors that can be compromised simultaneously. An example of this is email-based multifactor. If an attacker gains access to a user's password and can access their workstation where email is already logged in, they have easy access to any multifactor PIN that gets sent to the user's inbox.

Another requirement that's easy to miss is session timeouts. PCI requirement 8.2.8 mandates that any session that has been idle for more than 15 minutes must automatically time out and require re-authentication. For organizations that require users to log into multiple systems throughout the day, those re-authentications can be time consuming and frustrating enough that security teams never get around to enforcing them.

### Documenting Best Practices

There are some best practices that any organization can and should be practicing already and will set you up for success in the future.

Ensuring that you have internal policies and procedures is one. This may seem like an obvious must, but has been known to fall through the cracks. Jeremy Lacy, a senior consultant, and QSA breaks down exactly what this means in an article written for Forbes:

> "To achieve PCI compliance, your company must draft a detailed Information Security Policy (there is a whole section covering the requirements for that policy) and a complete set of policies to document secure practices across the systems environment, including documentation for antivirus, network configurations, physical security, and more. Then, you also must create step-by-step procedure documentation that details all processes carried out in the systems environment. Finally, someone that is qualified (e.g., CIO, IT director,

> security manager) must review and date stamp the documents annually to ensure the documents stay current."

A similar best practice that is often overlooked within the policies and procedures process itself is documenting significant changes. Experts recommend that every organization defines what constitutes "significant" and documents that clearly within their policies. It should detail how to implement said policies to the cardholder data environments.

### Understanding PCI DSS Compensating Controls

Compensating controls are an alternative solution or measures to a security or compliance requirement that is not possible for the organization to put in place in its original form. The PCI Council defines compensating controls as:

> "Compensating controls may be considered when an entity cannot meet a requirement explicitly as stated, due to legitimate technical or documented business constraints, but has sufficiently mitigated the risk associated with the requirement through implementation of other controls."

This simply means that any organization which cannot meet the requirements of PCI DSS must analyze and deploy similar levels of security measures that meet the specific standard requirements.

For designing and implementing a compensating control the organization must fulfill the criteria above, but let's break those down into more easily understandable terms:

**Meet the intent and rigor of the original PCI DSS requirement-** To fulfill these criteria the compensating control must provide the same level of security measure as the original control requirement. An example of this would be the PCI DSS requirements to maintain a firewall to protect cardholder data and the organization not having one. They would then need to have a compensating control that provides the same level of security for cardholder data to protect

it from attackers and unauthorized user access. The alternative measure must provide the **same type** of protection that would be provided by a firewall.

**Provide a similar level of defense as the original PCI DSS requirement-** While this criterion may sound redundant to the first one, this particular requirement is focused on the practical implication of the compensating control. If the original requirement is intended to provide a specific level of protection, and the compensating control is unable to match the protection of the initial requirement, the compensating control may be deemed ineffective by an auditor or quality assessor. Simply put, it is stating any compensating controls should be **equally strong and effective** as the original requirement.

**Be "above and beyond" other PCI DSS requirements (not simply in compliance with other PCI DSS requirements)-** For an organization to fulfill this requirement, they are required to ensure that if a compensating control is implemented and poses an additional risk, the compensating control must account for this risk as well – or runs the risk of being deemed invalid or ineffective.

**Be commensurate with the additional risk imposed by not adhering to the PCI DSS requirement.-** This control is often complicated, but in reality, it is quite simple. If your compensating control replaces one PCI requirement, it cannot be used as an alternate measure for any other PCI requirement. In other words, do not double-dip on compensating controls.

Once the compensating control is considered valid, organizations need to document its effectiveness in their environment. This documentation should include:

- Constraints List
- Objective
- Identified Risks
- Definition of Compensating Controls
- Maintenance

Ensuring that you can clearly and effectively answer these questions is critical when deploying compensating controls and for justifying them to a QSA.

In other words, prior to any compensating control being considered effective, your organization must complete an analysis to determine the risk associated with said controls and how you will mitigate any risks identified during the investigation. Documentation of the analysis is also essential to complete parts of the Report on Compliance (RoC) / Self-Assessment Questionnaire (SAQ) forms. These are two formal documents that are used to show that you are handling credit card information appropriately and are compliant with the PCI DSS, and will be required when Qualified Security Assessors conduct the annual audit.

### Don’t Roll The Dice with a QSA

Compensating controls are, in effect, a decision to debate a PCI auditor about whether your security controls are better than the PCI regulations as written. Being convincing in person is not enough, either; the auditor will look at the written RoC and SAQ documents you provide and decide whether or not the reasons listed are legitimate.

Whenever possible, play it safe and implement the controls as literally as you can. Additionally, keep in mind that while compensating controls are designed to assist organizations in their efforts to meet PCI DSS requirements, they are intended to be temporary. It is recommended that you replace these alternate measures with the original controls as quickly as possible.

## Section 2: Preparing for PCI 4.0

As of April 2022, the PCI SSC has released the final draft of PCI DSS 4.0, which will take effect in March 2024. One of the most notable changes in the requirements update is the clear alignment PCI SSC has made with NIST SP 800-63B Digital Identity Guidelines. PCI DSS 4.0 focuses heavily on fostering a zero-trust mindset and stronger authentication requirements. This includes mandating that multi-factor authentication (MFA) must be used for all accounts that have access to the cardholder data, not just administrators accessing the cardholder data environment.

PCI 4.0 doubles down on the importance of multi-factor authentication as protection for potential compromises. Security practices must evolve as threats change. The updated guidance is designed to address a variety of potential threats such as prompt bombing and social engineering. Authentication requirements are unchanged from PCI 3.2.1, where MFA requires two out of three distinct approved factors:

- Something you know, such as a password or passphrase.
- Something you have, such as a token device or smart card.
- Something you are, such as a **biometric element**.

There are, however, some substantial changes to how MFA is implemented.

**Section 8.1 Processes and mechanisms for identifying users and authenticating access to system components are defined and understood.**

**What's New:**

Section 8.1 starts by setting the expectations for security policies and operational procedures that are identified in Requirement 8.

> "Requirement 8.1.1 is about effectively managing and maintaining the various policies and procedures specified throughout Requirement 8. While it is important to define the specific policies or procedures called out in Requirement 8, it is equally important to

ensure they are properly documented, maintained, and disseminated."

" If roles and responsibilities are not formally assigned, personnel may not be aware of their day-to-day responsibilities and critical activities may not occur."

**What it Means:**

Make sure that all operational policies and procedures are documented, up to date, in use, and known to all affected parties. Roles and responsibilities for performing the activities in requirement 8 should also be assigned, understood, and documented.

**Section 8.2 User identification and related accounts for users and administrators are strictly managed throughout an account's lifecycle.**

Section 8.2 introduces the standard that All users are assigned a unique ID before access to system components or cardholder data is allowed. While this is not new, there has been new guidance provided for clarification.

**What's New:**

8.2.2 Individual user identity is confirmed before access to an account is granted access to any group, shared, or generic accounts.

8.2.3 Additional requirement for service providers only: Service providers with remote access to customer premises use unique authentication factors for each customer premises.

"Technologies such as multi-factor mechanisms that provide a unique credential for each connection could also meet the intent of this requirement."

8.2.7 Accounts used by third parties to access, support, or maintain system components via remote access are monitored for unexpected activity.

> 8.2.8 If a user session has been idle for more than 15 minutes, the user is required to re-authenticate to re-activate the terminal or session. This change aligns the PCI DSS requirements with that of NIST SP 800-63B.

**What it Means:**

This means that you will need to challenge your users for MFA far more often. Also, all the apps that agents log into will each need to be protected with MFA as well. This is challenging from an implementation perspective, but also, will impact the bottom line. For every hundred agents, 1000's of minutes each month will be spent on MFA challenges instead of calls.

> " When users walk away from an open machine with access to system components or cardholder data, there is a risk that the machine may be used by others in the user's absence, resulting in unauthorized account access and/or misuse."

**Section 8.3 Strong authentication for users and administrators is established and managed.**

Section 8.3 reiterates the importance of multi-factor authentication as protection for potential compromises. Approved factors for authentication are:

- Something you know, such as a password or passphrase.
- Something you have, such as a token device or smart card.
- Something you are, such as a **biometric element.**

**What's New:**

> 8.3.3 User identity is verified before modifying any authentication factor. Methods to verify a user's identity include a secret question/answer, knowledge-based information, and calling the user back at a known and previously established phone number.

This addition could mean credential resets will be susceptible to more scrutiny.

8.3.4 Invalid uthentication attempts are limited by:

- Locking out the user ID after not more than 10 attempts.
- Setting the lockout duration to a minimum of 30 minutes or until the user's identity is confirmed.

The addition of 8.3.4 is particularly interesting given the increase in prompt bombing, a social engineering technique designed to leverage MFA fatigue to gain access to a target's account.

8.3.6 If passwords/passphrases are used as authentication factors to meet Requirement 8.3.1, they meet the following minimum level of complexity:

- A minimum length of 12 characters (or IF the system does not support 12 characters, a minimum length of eight characters).
- Contain both numeric and alphabetic characters.

8.3.10.1 Additional requirement for service providers only: If passwords/passphrases are used as the only authentication factor for customer user access (i.e., in any single-factor authentication implementation) then either:

- Passwords/passphrases are changed at least once every 90 days, OR
- The security posture of accounts is dynamically analyzed, and real-time access to resources is automatically determined accordingly.

**What it Means:**

Section 8.3 is all about strong authentication factors to prevent and minimize the risk of compromise. Ensuring that your organization has at minimum 2/3 MFA factors, complex passwords with a 90-day rotation in non-CDE, and dynamic analysis of account security in accordance with NIST Special Publication 800-207 Zero Trust Architecture.

" Having physical and/or logical controls (for example, a PIN, biometric data, or a password) to uniquely authenticate the user of the account will prevent unauthorized users from gaining access to the user account through use of a shared authentication

> factor."

**Section 8.4 Multi-factor authentication (MFA) is implemented to secure access into the cardholder data environment.**

Section 8.4 as it exists in 4.0 now focuses on MFA implementation across all accounts to secure access into the CDE.

**What's New:**

8.4.2 clearly states MFA is implemented for all access into the cardholder data environment, and step-up MFA is required.

> "8.4.1 Administrative access to the CDE cannot be obtained by the use of a single authentication factor."

> 8.4.2 MFA is implemented for all access into the CDE.
> "If an individual first connects to the entity's network via remote access, and then later initiates a connection into the CDE from within the network, per this requirement the individual would authenticate using MFA twice,"

Section 8.4 in PCI DSS 3.2.1 focused primarily on the documentation and communication of authentication policies. The updated guidance provided in 4.0 clarifies that using one factor twice (for example, using two separate passwords) is not considered multi-factor authentication.

**What it Means:**

This requirement clearly states MFA is implemented for all access into the cardholder data environment, and step-up MFA is required. Previously, MFA was required for individual non-console administrative access and all remote access to the cardholder data environment, and network access as well.

Section 8.5 Multi-factor authentication (MFA) systems are configured to prevent misuse.

Section 8.5 previously focused on group, shared, or generic IDs, passwords, or authentication methods which are now included in section 8.2. 8.5 now provides guidance on multi-factor authentication best practices, system configurations, and how to prevent misuse.

**What's New:**

8.5.1 also addresses the risk of poorly configured MFA systems and ways that poor configuration can lead to the system being bypassed by attackers. MFA systems are implemented as follows:

- The MFA system is not susceptible to replay attacks.
- Success of all authentication factors is required before access is granted.

**What it Means:**

Properly configuring and deploying solutions is going to be much more strictly assessed. It will be critical to ensure that MFA systems are configured properly and that any previously shared authentication methods are aligned with the new guidance. Remember that success of all the authentication factors will be required in order to gain access.

**Section 8.6 Use of application and system accounts and associated authentication factors is strictly managed.**

8.6 shifts the focus from the implementation of MFA to the management of system accounts and associated authentication factors.

**What's New:**

Password complexity has become stricter in PCI 4.0 but rotation requirements have relaxed. The new password policy requirements are as follows:

8.3.6 If passwords/passphrases are used as authentication factors, they meet the following minimum level of complexity:

- A minimum length of 12 characters (or IF the system does not support 12 characters, a minimum length of eight characters).
- Contain both numeric and alphabetic characters.

8.6.3 Passwords/passphrases for any application and system accounts are protected against misuse as follows:

- Consider password changes at least once a year,
- a password/passphrase length of at least 15 characters, and
- complexity for the passwords/passphrase of alphanumeric characters, with upper- and lower-case letters, and special characters.

**What it Means:**

You'll need to enforce at least 12 but probably 15 character alphanumeric passwords. These will rotate once a year, rather than once a quarter.

If you're not already implementing complex passwords, this is probably going to be a major lift to get all your systems to implement the change, and then also, have all your users reset their credentials to meet the new standards. The bad news is that this process will almost certainly result in a heavy IT workload over the following few weeks with spiking credential resets as users struggle to adapt. The good news, however, is that once the initial flood of helpdesk tickets dies down, the relaxed rotation period of one year will probably result in a 75% reduction in credential resets at the helpdesk over time.

If you stagger the rotation period across your users, you can avoid another huge spike in ticket loads next year when everyone's credentials reset at the same time and the new complex passwords drive up locked accounts again. Our recommendation is therefore to get started on this early and roll it out to users' tranches evenly over a year.

For outsourced contact centers and business process outsourcing (BPOs) specifically, there is an extra sub-requirement for credentials:

> 8.3.10.1 Additional requirement for service providers only: If passwords/passphrases are used as the only authentication factor for customer user access (i.e., in any single-factor authentication implementation) then either:
>
> - Passwords/passphrases are changed at least once every 90 days, OR
> - The security posture of accounts is dynamically analyzed, and real-time access to resources is automatically determined accordingly.

**Conclusion:**

The release of updated guidance means there are 21 months to review, plan, and implement updated security policies and procedures. With stronger authentication requirements being at the core of PCI DSS 4.0, it is critical that organizations review the section 8 requirements and develop a plan to meet them.

As recent breaches against contact centers have informed the new PCI guidance, strict adherence to PCI 4.0 is an organization's best bet to protect against sophisticated threat actors and the tools they most commonly use.

## Section 3: Biometric MFA is the Only Way Forward

### Contact Center MFA - Mission Impossible

Contact center facilities face a unique and pressing challenge: maintaining PCI compliance by implementing identity security measures such as multi-factor authentication. In most secured facilities, employees are highly restricted when it comes to what can and cannot enter the workspace. Cell phones, bags, and writing utensils are strictly prohibited due to the nature of the information they work with, such as PII (personally identifiable information) like credit card details. As threats evolve, so must security practices.

With phones banished from contact center floors, it became difficult to follow PCI DSS MFA Guidance V1, which states "MFA requires at least two of the three authentication methods described in PCI DSS Requirement 8.2."

- Something you have, like a mobile phone or hard token
- Something you know, such as a password, and
- Something you are, such as a biometric.

### Something You Have

While  contact centers can theoretically combine "something you have" and "something you are," in practical terms both mobile and hard-token based MFA tools are off the table.

Hard tokens are both expensive and high maintenance. It is no secret that contact centers have exceptionally high churn, meaning that many of those costly hard token devices are not making their way back into the company's hands. Replacing them costs money, tracking them down costs money, and managing them (assigning, unassigning, and monitoring) requires time and effort.

The adoption of hard tokens also brings the necessity for IT support for when they don't work, get lost, or the batteries die. According to a study done by Veridium, "Tokens and smartcards can cost companies millions, regardless of industry".  In the same research conducted by

Veridium, they reviewed the monetary impact of 3 organizations across 3 industries, and the results showed that security hardware, support for said hardware, and friction of inefficient security measures is costing organizations well into the millions.

Consider the scenario in which an employee quits or gets fired. Your organization has a choice to make: try to get the hard token back, or write it off and purchase a new one. While it would obviously be preferable to recycle the hardware, it turns out that convincing an outgoing employee to go through the effort of mailing the token back can be outright impossible. Even if they are willing to send it back, the process of reassigning the key to a new user can be so time consuming, confusing, and frustrating that many IT departments simply give up and eat the cost of issuing a new token.

This means that for a 100-employee team, with industry average 150% turnover, an organization actually ends up purchasing more than 150 keys per year! This is not only expensive, but also profoundly wasteful. Throwing thousands of hardware tokens away each year is not sustainable from either an environmental standpoint, or a business one.

With "something you have" no longer a practical option due to the physical control of restricting agents from having mobile devices on the floor or at their workstation and the overwhelming cost of hard tokens, that leaves a combination of "something you know" and "something you are."

**Something You Are**

Over the past several years, and particularly over the last few months, biometric factors have rapidly increased in popularity. This is both out of necessity to adopt innovative solutions, but also because of the initiatives of the OMB and the Biden administration to proactively move towards true zero trust in both the private and public sectors.

While PCI guidance recommends biometric authentication, there is no specific language on what exactly is considered a biometric factor. Luckily, there is a clear precedent: in the February 2017 Information Supplement Multi-factor Authentication section on SMS, PCI says:

"PCI DSS relies on industry standards—such as NIST, ISO, and ANSI—that cover all industries, not just the payments industry. While NIST currently permits the use of SMS, they have advised that out-of-band authentication using SMS or voice has been deprecated and may be removed from future releases."

Because PCI DSS relies on NIST, ISO, and ANSI, we can look to their definition of a biometric for guidance. The National Institute of Standards and Technology defines biometrics as "Automated recognition of individuals based on their biological and **behavioral** characteristics,"-NIST Special Publication 800-63.

In simple terms, biometrics measure something that is intrinsically part of an individual. This includes how a user behaves when they interact with a computer.

**The Twosense Effect**

The most important part of resolving the fundamental issue within contact center facilities is finding the proper vendor to partner with. Developed in partnership with the US Department of Defense, Twosense has created a cutting-edge, software-only multi-factor authentication designed specifically for contact centers to meet PCI compliance. Deploying behavioral biometrics allows organizations to breeze through PCI audits and cybersecurity insurance checks with NIST approved technology that is already PCI 4.0 compliant.

Identity verification via biometrics means no mobile app, no hardware tokens, and no additional equipment like thumbprint readers. Because users are automated out of the multi-factor process, Twosense MFA also meets the phishing-resistant MFA guidance set forth by the OMB and Biden Administration's "Moving the U.S. Government Towards Zero Trust Cybersecurity Principles" initiative. Additionally, BPO organizations can also close more security conscious customers by advertising that they use biometric authentication to secure agents' access to their networks.

Without the need to purchase and continually replace hard tokens, Twosense saves both money and IT departments' valuable time. Twosense does not require organizations to assign, reassign, or manage seats or devices. By design, Twosense only counts people actively using

the software in the last 30 days. This helps reduce significant friction for administrators and reduces wasteful spending.

By removing the frequent interruptions associated with MFA challenges, managers and agents are more time-efficient on and off of customer service calls. On average, Twosense customers save 40 minutes a month per agent by eliminating identity security friction. This reduces call waiting times, and resolution times, and allows for agents to serve more customers throughout the day.

Implementing behavioral biometrics such as Twosense Passive MFA or Continuous MFA into contact centers' identity security postures enables organizations to do what was previously impossible: deploy MFA everywhere, to every user without increasing user friction or negatively impacting their ability to serve customers.

**The Way Forward**

The reality is that BPO contact centers have historically been dealt a losing hand when it comes to implementing effective and compliant multi-factor authentication in their call centers. This is why Twosense is dedicated to solving the problem contact centers face: with restricted devices, work-from-home agents, and PCI DSS compliance to meet, behavioral biometric multi-factor authentication is the only available solution to meeting and maintaining PCI compliance for contact centers.

AFGE

**“MFA is something everyone loves to hate, but it’s necessary and people get it. With Twosense we are able to make that necessary evil a little less evil.”**

**-Taylor Higley, Director of Information Services, American Federation of Government Employees**