Federal Trade Commission
Privacy Impact Assessment

Okta Customer Identity and Access Management

(Okta CIAM/Okta)

June 2021

Table of Contents

1 System Overview

1.1 Describe the project/system and its purpose.

The FTC utilizes the Okta Customer Identity and Authentication Management (Okta CIAM or Okta) identity cloud platform to secure and validate external user identities. Okta has implemented the following features to support the registration of users for custom applications built into the ServiceNow platform.

Single Sign On (SSO) – SSO is a technology that combines different application login screens into one. With SSO, external users must first complete the Okta registration process; once registered, users only need to enter their login credentials (username, password) one time on a login page to access the ServiceNow applications.

Security Markup Language (SAML) – Okta utilizes SAML to integrate with the FTC SSO. SAML is an XML-based standard for exchanging authentication and authorization data between security domains. Okta exchanges information with the ServiceNow SAML plugin, which supports SSO-based authentication.

Multi-Factor Authentication (MFA)/ Okta Verify – MFA, also known as two-step verification, requires users to enter more than one set of credentials to authenticate their account. Okta Verify is an MFA factor and authenticator application developed by Okta that is used to confirm the user's identity when they sign into their Okta account. After the external user installs Okta Verify on their primary device, they can then verify their identity by approving a push notification or by entering a one-time code. Okta is used to verify identity only and act as a gateway to the FTC ServiceNow applications.

These features were chosen to provide a high level of identity management security to ensure that the users accessing the system are thoroughly authenticated each time they enter the system.

External User Registration – When requesting access to the ServiceNow applications system, an external user receives an email prompting them to register an account using a hyperlink provided within the email. Clicking on the hyperlink takes the user to the Okta customer registration web page. The user must fill in the following fields to complete the registration: first name, last name, business email, phone number, and company name. Upon successful registration, the user is presented with a confirmation page. The external user is also notified that a follow up email with additional steps to complete the registration process will be sent to the email address they provided. The post registration email contains further instructions for the user to create an account password and set up MFA; this includes choosing security questions for additional authentication purposes.

1.2 What specific legal authority allows for the collection, maintenance, or dissemination of information for this project/system?

The Federal Trade Commission Act, 15 U.S.C. §§ 41-58, the Commission Rules of Practice, and other statutes and regulations enforced by the agency authorizes the FTC to collect the information that is sent, received, and maintained by the Okta platform. In addition, collection of this information for purposes of managing and securing individuals' system access is authorized under the Federal Information Security Modernization Act, 44 U.S.C. §§ 3551 et seq.

2 Data Type, Sources, and Use

2.1 Specify in the table below what types of personally identifiable information (PII)[1] may be collected or maintained in the system/project. Check <u>all</u> that apply.

PII Elements: This is not intended to be an exhaustive list. Specify other categories of PII as needed.		
☒ Full Name	☐ Biometric Identifiers (e.g., fingerprint, voiceprint)	☒ User ID
☐ Date of Birth	☐ Audio Recordings	☐ Internet Cookie Containing PII
☐ Home Address	☐ Photographic Identifiers (e.g., image, x-ray, video)	☐ Employment Status, History, or Information
☒ Phone Number(s)	☐ Certificates (e.g., birth, death, marriage, etc.)	☐ Employee Identification Number (EIN)
☐ Place of Birth	☐ Legal Documents, Records, Notes (e.g., divorce decree, criminal records, etc.)	☐ Salary
☐ Age	☐ Vehicle Identifiers (e.g., license plates)	☐ Military Status/Records/ ID Number
☐ Race/ethnicity	☐ Financial Information (e.g., account number, PINs, passwords, credit report, etc.)	☒ IP/MAC Address
☐ Alias	☒ Geolocation Information	☐ Investigation Report or Database
☐ Sex	☐ Passport Number	☐ Driver's License/State ID Number (or foreign country equivalent)
☒ Email Address		☒ Other *(Please Specify)*: Login and Log-out Date Time, Security questions for password reset/ PIN/Password/ Company Name_____
☐ Work Address		
☐ Taxpayer ID		
☐ Credit Card Number		
☐ Facsimile Number		
☐ Medical Information		
☐ Education Records		
☐ Social Security Number		
☐ Mother's Maiden Name		

2.2 What types of information other than PII will be collected, disseminated, or maintained by the project/system? Provide a general description below and be sure to include all data elements.

Not applicable. The system does not collect any additional non-PII data.

[1] Per OMB Circular A-130, personally identifiable information (PII) means information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual.

2.3 What is the purpose for collection of the information listed above?

The information listed above is collected by Okta CIAM to validate user identity before granting users access to the ServiceNow application. The PII collected is used to create the registration email message generated by ServiceNow. The registration email is sent to the email address provided by the user.

Adaptive Multi-Factor Authentication allows the system to validate the identity of external users by providing the ability to create security questions, passwords, and utilize Okta Verify. Adaptive Multi-Factor Authentication also provides FTC with the ability to enforce contextual access management features, such as location verification, geo-location, impossible travel, new device recognition, new IP address, specified IP zones, and network anonymizers.[2]

FTC manages all external users, groups, and devices within the Okta CIAM Universal Directory, which contains a comprehensive list of all authorized users.

2.4 What are the sources of the information in the system/project? How is the information collected?

Source of Data	*Type of Data Provided & How It Is Collected*
External Users	An external user will receive an email requesting that the user register via Okta CIAM using a unique hyperlink. By clicking on the hyperlink, the user will be presented with a customer registration web page. The page contains the following fields to be completed: first name, last name, business email, phone number, and company name. A Rules of Behavior link is also available on this page. Upon successful registration, the user is presented with the registration confirmation page. The external user is also notified that an email with additional steps to complete the registration process will be subsequently sent to their business email address. After receiving the post registration email, the user must follow instructions provided to set up a uniqe password and MFA.

[2] Impossible travel refers to logging into the system from what appear to be two distinct geographic locations, which would not be possible given the distance and time of logins. Specified IP zones enable Okta administrators to define network perimeters around a set of approved IPs. Network anonymizers attempt to make activity on the Internet untraceable by accessing the internet on the user's behalf and hiding the user's information. By setting up or customizing dynamic zones, Okta CIAM is able to limit access to only those recognized proxy servers (network anonymizers) and block unauthorized proxy servers, if configured to do so.

3 Data Access and Sharing

3.1 In the table below, specify the systems/applications and groups (both FTC and non-FTC) that will have access to or share data in the system/project.

Data Will Be Accessed By and/or Provided To:	*How and Why the Data Will Be Accessed/Shared*
FTC Staff and Contracted support for OCIO Hosted Services in support of application modernization ITSS BPA TO5, currently 1901 Group	Information stored by Okta is accessible by FTC Okta CIAM administrators. Administrators need the ability to access and/or correct PII required for the use of FTC applications that use Okta for authentication purposes.
Okta CIAM Customers (external users)	Once logged into Okta CIAM, users can access their account page and edit their personal information. This includes their name, email address, and mobile phone number. They can also select the preferred method for account verification by choosing either "Okta Verify" or "Voice Call Authentication."
Okta CIAM Administrators	For troubleshooting and maintenance purposes, authorized Okta CIAM administrators have access to data.

3.2 Do contractors and/or third-party service providers have access to data in the project/system? If yes, explain what privacy requirements are in place to ensure that data is properly protected.

Yes, FTC Contracted support for OCIO Hosted Services in support of application modernization ITSS BPA TO5, currently 1901 Group have access to data in the system. Contractors must use FTC issued laptops to access the system using their Personal Identity Verification (PIV) cards. All FTC contractors are required to sign non-disclosure agreements (NDA), complete security and privacy training prior to obtaining access to any FTC systems, and annually thereafter to maintain network access and access to those systems.

Okta makes multiple investments to ensure external data is secure and available. External user data, and access to it, is isolated at the customer level within Okta's data layer. Data is stored in an encrypted manner in the Amazon Web Services (AWS).

Okta requires that all access to its infrastructure, application, and data be controlled based on business and operational requirements. Following the principles of segregation of duties and least privilege, code changes and maintenance are split between multiple teams. In all cases, administrative access is based on the concept of least privilege; users are limited to the minimum set of privileges required to perform their required job functions.

3.3 If you answered "yes" to 3.2, describe the privacy incident response plan maintained by the contractor's organization or third-party service provider.

FTC contractors with access rights to the Okta CIAM application are subject to the same rules and policies as FTC staff, including adherence to the FTC Breach Notification Response Plan. Okta CIAM is also be subject to the FTC Incident Response plan, which includes measures to prevent, detect, contain, eradicate and recover from breaches that would include personal identity information (PII).

Okta is a Federal Risk and Authorization Management Program (FedRAMP) authorized system providing Software as a Service to the public cloud. Okta's Incident Response procedures have been evaluated by a Third-Party Assessment Organization (3PAO), and Okta's assigned controls meet FedRAMP compliance standards. The Okta Incident Response Team (IRT) is responsible for developing the facts relating to an incident and determining the appropriate response. If the incident triggers the FedRAMP incident response requirements, the IRT must comply with the classification, incident management and coordination procedures outlined in the Okta FedRAMP Incident Response Plan. Okta will communicate with the FTC as needed based on the incident and if FTC user information is impacted.

4 Notice and Consent

4.1 How are individuals provided with notice prior to the collection of their PII? If notice is not provided, explain why.

☒ Notice is provided via (*check all that apply*):
- ☒ Privacy Act Statement (☒ Written ☐ Oral)
- ☐ FTC Website Privacy Policy
- ☐ Privacy Notice (e.g., on Social Media platforms)
- ☐ Login banner
- ☒ Other (*explain*): Every external user is required to sign the FTC Rules of Behavior (ROB) prior to use of the application.

☐ Notice is not provided (explain): _____

4.2 Do individuals have the opportunity to decline to provide information or to consent to particular uses of their information (other than required or authorized uses)?

Yes. In order to access the ServiceNow applications system, users must register and create an account via Okta CIAM. If they choose not to create an account, they will not be able to electronically file using ServiceNow applications. The user must provide a valid email address (along with other required PII) to validate their account and agree to the Rules of Behavior (RoB) during the registration process.

4.3 Are there procedures in place to allow individuals access to their personally identifiable information? Explain.

Yes. Users have the ability to verify and edit their own personal information. Once logged into Okta, the user can go to "Settings" and edit their personal information. An additional "Extra Verification" section also allows the user to select either "Okta Verify" or "Voice Call Authentication" to validate their account.[3]

4.4 Are there procedures in place to allow individuals the ability to correct inaccurate or erroneous information? What is the process for receiving and responding to complaints, concerns, or questions from individuals? Explain.

As mentioned above in 4.3, the individual registering an account on Okta CIAM has the ability to edit their information by accessing the "Settings" section of their account. Once on the "Settings" page, the user can click on the "Edit" button and making any changes to their name, email address, and phone number. There is also a "Extra Verification" option which allows the user to choose between "Okta Verify" or "Voice Call Authentication" to validate their account.

An individual may make a Privacy Act request to the FTC for access to additional information maintained about them in the Okta CIAM application. See Commission Rule 4.13 (Privacy Act request procedures). The FTC, however, does not have the ability to correct any information provided by users and relies on the individual to input accurate information, as noted above. Access to the information under the Privacy Act may be subject to certain exemptions. See Commission Rule 4.13(m). Individuals may also file Freedom of Information Act (FOIA) requests for agency records about them (if they are not exempt from 6 disclosure to them under those laws). Additionally, individuals may contact the FTC with any complaints, questions or concerns via phone or email available on www.ftc.gov or contact the Chief Privacy Officer directly.

5 Data Accuracy and Security

5.1 Are there procedures in place to ensure that the information maintained is accurate, complete, and up-to-date?

The FTC does not have the ability to verify whether the information a registrant has provided is accurate or up-to-date. Therefore, it is incumbent upon the person registering for an account with Okta CIAM to ensure that the information they have provided is accurate and up to date. See Section 4.3. and 4.4.

[3] For more information, refer to Okta's Privacy Policy: https://www.okta.com/privacy-policy/#x-your-information-choices-19.

5.2 Are there administrative procedures and technical safeguards in place to protect the data in the system/project? What controls are in place to ensure proper use of the data? Please specify.

Yes. Okta CIAM can currently be accessed by FTC staff and FTC contractors. Contractors and Okta administrative users must sign confidentiality and nondisclosure agreements, and, in some cases, are required to undergo additional security clearance procedures.

Okta operates under a shared security responsibility model. Okta is responsible for the security of the cloud platform and underlying infrastructure, while the FTC is responsible for the security in the cloud, such as granting correct permissions, disabling accounts for former employees, enforcing multi-factor authentication, properly configuring and monitoring authentication policies, reviewing system logs, and monitoring Okta tenants for attacks. All Okta data is encrypted both at rest and in transit. Additionally, Okta uses organization-level encryption to protect sensitive data, such as authentication credentials and certificates.

User PII stored within Okta is accessible by a limited number of people based on their roles. Data is accessed by Okta-managed systems over secure communication channels outside of Okta physical locations. Remote access is not permitted from personal devices, nor can PII be exported to removable devices.

Additional controls include password length and complexity requirements, password expirations every 90 days, and account lockout (for 30 minutes) after three unsuccessful login attempts. All Okta CIAM users are required by administrative security policy to select either "Okta Verify" or "Voice Call Authentication" to enable multi-factor authentication. Okta CIAM also uses additional measures to track unusual activity, like when a user requests access from an anomalous location, IP, or device.

5.3 Is PII used in the course of system testing, training, or research? If so, what steps are taken to minimize and protect PII during this process?

Not Applicable. PII is not used in the course of system testing, training, or research.

6 Data Retention and Disposal

6.1 Specify the period of time that data is retained in the system/project. What are the specific procedures for disposing of the data at the end of the retention period?

To the extent that records maintained in the Okta platform constitute records without the custody or control of the FTC, such records shall be retained and destroyed in accordance with schedules and procedures issued or approved by the National Archives and Records Administration (NARA). The disposition of general technology and information system

security records are covered by NARA disposition instructions in General Records Schedules (GRS) 3.1 and 3.2.

Okta application generated system data, as well as reporting based on log data older than three months is automatically removed. Okta service backup data is automatically purged six months after it is first generated.

7 Website Privacy Evaluation

7.1 Does the project/system employ the use of a website? If so, describe any tracking technology used by the website and whether the technology is persistent or temporary (e.g., session cookie, persistent cookie, web beacon). Describe the purpose of using such tracking technology.

Yes, Okta CIAM employs the use of a website that uses tracking technology known as cookies. These cookies are necessary for the website to function and cannot be switched off. They are usually only set in response to actions made by the user, which amount to a request for services, such as setting their individual privacy preferences, logging in or filling in forms. The user can set their browser to block or alert them about these cookies, but some parts of the site will not work if they opt for this action. These cookies do not store any personally identifiable information.

Functional cookies enable the website to provide enhanced functionality and personalization. They may be set by Okta or by third party providers whose services have been added to Okta's pages. If the user does not allow these cookies, then some or all of these services may not function properly.

Performance cookies allow Okta to count visits and traffic sources so that Okta can measure and improve the performance of its site. They help Okta to figure out which pages are the most and least popular and see how visitors move around the site. All information these cookies collect is aggregated and anonymous.

Targeting cookies may be set through the Okta site by its advertising partners. They may be used by those companies to build a profile of the user's interests and show users relevant adverts on other sites. They do not store directly personal information but are based on uniquely identifying the user's browser and internet device. The user can opt out of allowing these cookies, and they will experience less targeted advertising.

If the user does not wish to have cookies set on their device for any reason, they may opt out of all cookies via their browser. The above activities are conducted and controlled by Okta, not the FTC. For more information about Okta's Cookie Policy, go to https://www.okta.com/cookies-policy/.

8 Privacy Risks and Evaluation

8.1 Considering the type of information collected and sources of collection, what privacy risks were identified and how were these risks mitigated?

Risk	*Mitigation Strategy*
Misuse of data by authorized users	Prior to receiving access to the FTC's network, all users must agree to the FTC Rules of Behavior, which includes consenting to monitoring and restrictions on data usage.
Unauthorized system access	All FTC users must have an FTC account and government issued PIV card to access Okta CIAM. The FTC utilizes a combination of technical and operational controls to reduce risk in Okta CIAM, such as encryption, passwords, audit logs, firewalls, malware identification, and data loss prevention policies. As a FedRAMP-approved cloud service provider, Okta CIAM undergoes regular reviews of its security controls. External users will be required to authenticate using two-factor authentication: username/password and passcode delivered to user (voice or token authenticator app on their smartphone).
Data leakage	Non-FTC ServiceNow system administrators are not allowed to review, audit, transmit, or store FTC Okta CIAM registration data, which minimizes privacy risks from the vendor source.
Unwanted eavesdropping	Users interact with Okta CIAM over the TLS protocol (https), an authenticated protected channel.

8.2 Does the project/system employ the use of automated privacy controls or enhanced capabilities designed to support privacy? Explain.

All Okta CIAM users are required by administrative security policy to select either Okta Verify or Voice Call Authentication to enable multi-factor authentication. Okta CIAM also uses additional measures to track unusual activity, such as when a user requests access from an anomalous location, IP, or device. Okta CIAM security engineers review and report weekly on Okta usage, application usage, suspicious activity, and system logs to the Okta CIAM ISSO assigned by FTC.

8.3 Has a Privacy Act System of Records Notice (SORN) been published in the Federal Register for this system/project? If so, list the applicable SORN(s).

Not applicable. The Okta CIAM system is controlled and operated by a third party and, although it is integrated into the FTC's ServiceNow platform for the purpose of authenticating and granting authorized users access to FTC's systems, Okta itself is not considered to be an agency records system.

To the extent, if any, that the FTC collects and maintains agency records about individuals for identification and access and security purposes, such records would be covered by FTC VII-3 (computer user identification and access records). See https://www.ftc.gov/site-information/privacy-policy/privacy-act-systems.

8.4 How does the project/system ensure that the information is collected, used, stored, or disseminated in accordance with stated practices in this PIA?

The administrative and technical controls described in section 5.2 of this document provide assurance that the collection, use, and maintenance of the information will be conducted as described in this PIA. This PIA aligns with the FTC's existing privacy policies and procedures and is subject to periodic review by the Office of the Chief Privacy Officer (OCPO), in consultation with relevant program staff and other relevant agency officials.