WE ARE YOUR DOL

NEW YORK STATE OF OPPORTUNITY. Department of Labor

Instrukcja konfiguracji uwierzytelniania wieloczynnikowego (MFA)

Stan Nowy Jork rozpoczął stosowanie uwierzytelniania wieloczynnikowego (MFA) w niektórych swoich aplikacjach publicznych. MFA to sposób, który pomaga zapewnić bezpieczeństwo i ochronę Twojego konta. Wymaga to drugiego czynnika udowadniającego (poza samym hasłem), że jesteś tym, za kogo się podajesz. Jeśli korzystasz z aplikacji chronionej MFA, nawet jeśli ktoś odgadnie lub ukradnie Twoje hasło, nadal nie będzie mógł się zalogować bez Twojego drugiego czynnika. Podczas gdy hasło to coś, co znasz, drugi czynnik to coś, czym jesteś (zwykle odczytywane przez urządzenie biometryczne) lub coś, co masz.

Porada: Zaleca się skonfigurowanie więcej niż jednej metody uwierzytelniania wieloczynnikowego.

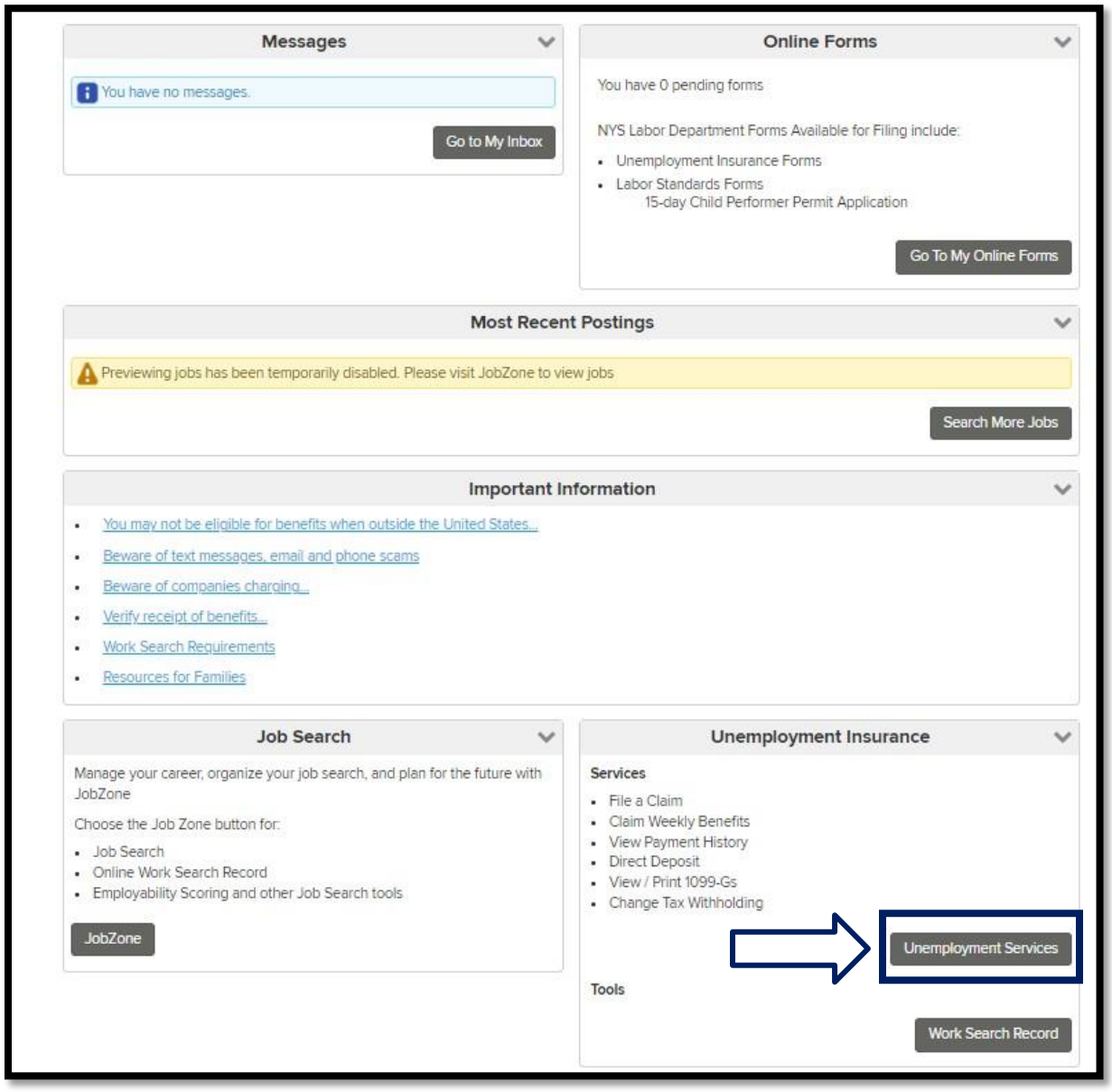
Porada: Jeśli będziesz konfigurował metodę uwierzytelniania wieloczynnikowego, która wykorzystuje aplikację na telefon (Okta Verify lub Google Authenticator), pobierz aplikację przed kliknięciem przycisku Setup/Konfiguruj na stronie przeglądarki „Set up multifactor authentication/Konfiguruj uwierzytelnianie wieloczynnikowe”. Dwie metody uwierzytelniania wieloczynnikowego, które wykorzystują aplikacje, to Okta Verify i Google Authenticator. Aby pobrać aplikację już teraz, kliknij tutaj dla urządzeń z systemem Android, a tutaj dla urządzeń Apple.

UWAGA: Wszystkie zrzuty ekranu pochodzą z monitora komputera, chyba że zostały zrobione za pomocą telefonu komórkowego.

Indeks

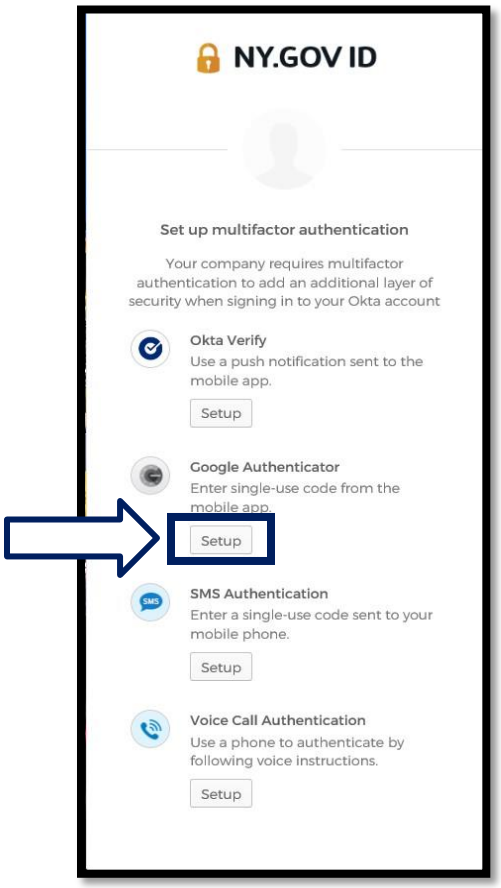
Konfiguracja uwierzytelniania wieloczynnikowego przez Google Authenticator

Jeśli nie jesteś jeszcze zapisany do MFA, zostaniesz poproszony o zapisanie się po zalogowaniu się do Labor Online Services i kliknięciu przycisku „Unemployment Services/Usługi dla osób bezrobotnych”.



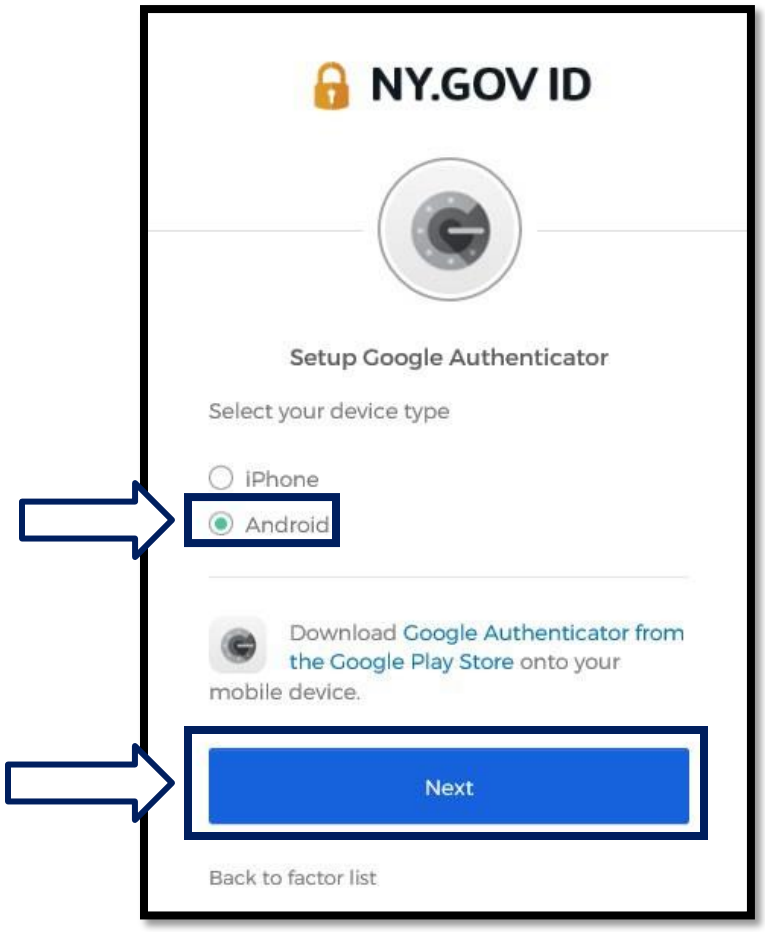
Na ekranie komputera pojawi się ekran z prośbą o skonfigurowanie uwierzytelniania wieloczynnikowego.

1. Na swoim smartfonie pobierz aplikację Google Authenticator.
2. Na ekranie komputera kliknij opcję Setup/Konfiguracja w obszarze Google Authenticator, aby rozpocząć proces konfiguracji.



3. Na monitorze komputera otworzy się nowy ekran. Wybierz iPhone lub Android w zależności od urządzenia. Jeśli masz tablet Apple, wybierz iPhone.

   Jeśli masz urządzenie z systemem Android, zobaczysz:



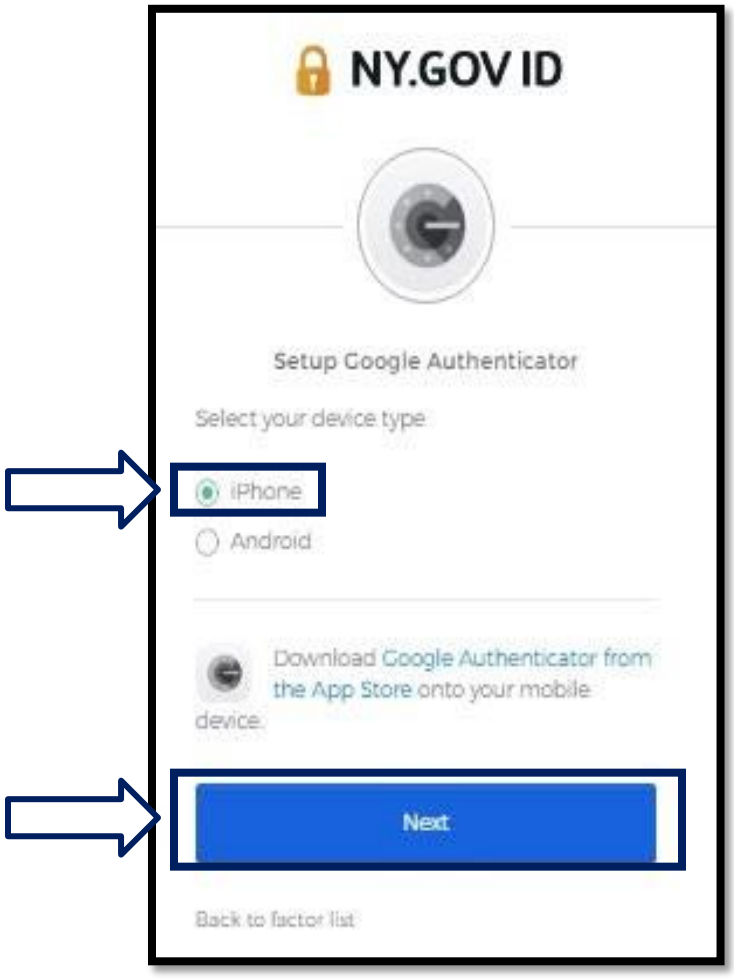
   Zostaniesz poinstruowany, aby pobrać aplikację Google Authenticator ze sklepu Google Play. Jeśli jeszcze tego nie zrobiłeś, powinieneś pobrać tę aplikację już teraz.

   Kliknij tutaj, aby uzyskać wskazówki, jak pobrać aplikację Google Authenticator na urządzenie z systemem Android.

4. Kliknij przycisk Next/Dalej.

   Kliknij tutaj, aby kontynuować.

Jeśli masz urządzenie iPhone, zobaczysz:



Zostaniesz poinstruowany, aby pobrać aplikację Google Authenticator ze sklepu App Store. Jeśli jeszcze tego nie zrobiłeś, powinieneś pobrać tę aplikację już teraz.

Kliknij tutaj, aby uzyskać wskazówki, jak pobrać aplikację Google Authenticator na urządzenie Apple.

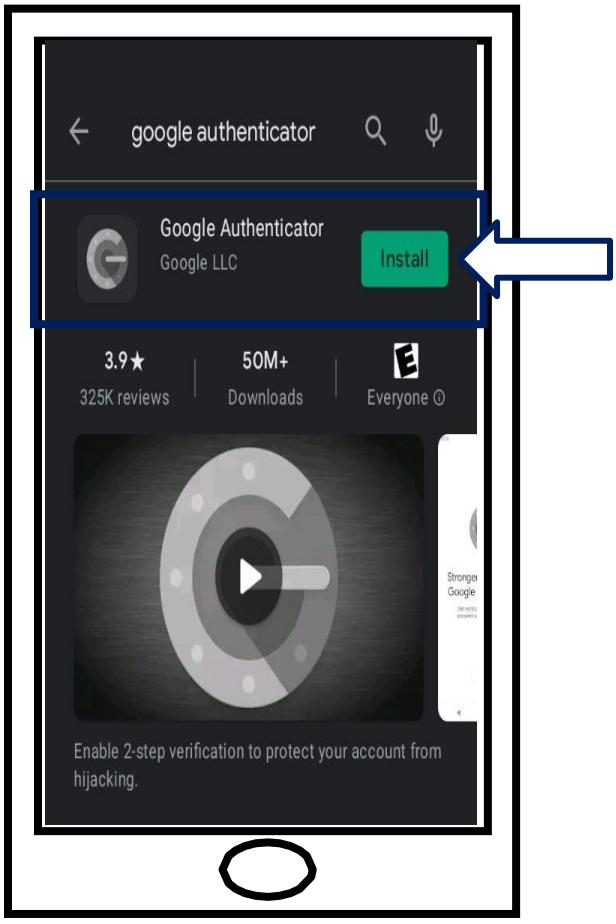
5. Kliknij przycisk Next/Dalej.

Wskazówki dotyczące pobierania aplikacji Google Authenticator na urządzenie z systemem Android.

6. Na swoim smartfonie lub tablecie przejdź do Google Play. Upewnij się, że na Twoim smartfonie lub tablecie działa najnowsza wersja systemu operacyjnego (OS).

7. W sklepie Google Play wyszukaj aplikację Google Authenticator.

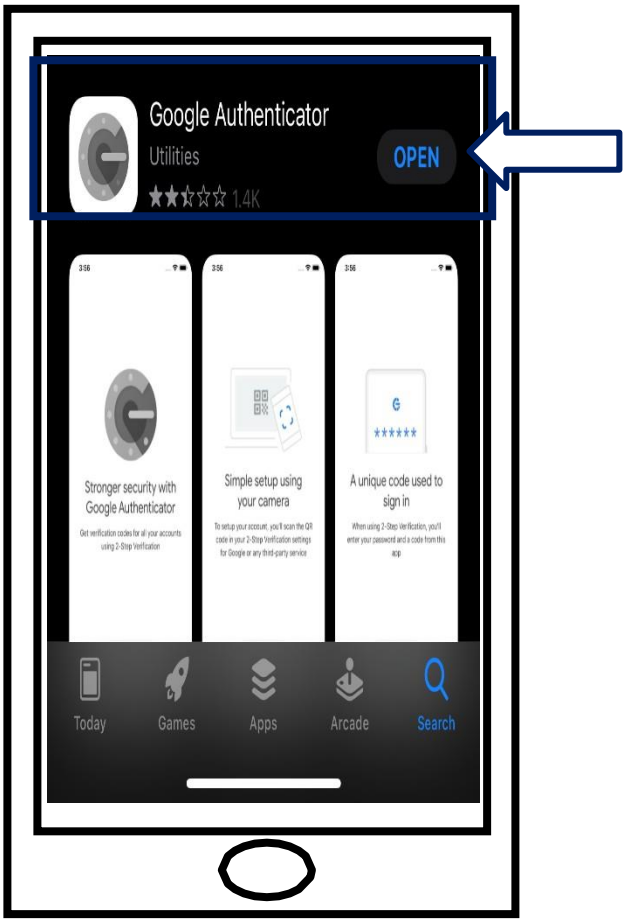
8. Po znalezieniu aplikacji, pobierz i zainstaluj ją na swoim smartfonie lub tablecie. *(UWAGA: Aplikacja może wyglądać nieco inaczej w zależności od wersji telefonu)*



[Kliknij tutaj, aby wrócić do strony głównej]

Wskazówki dotyczące pobierania aplikacji Google Authenticator na urządzenie Apple.

9. Na swoim smartfonie lub tablecie przejdź do App Store. Upewnij się, że na Twoim smartfonie lub tablecie działa najnowsza wersja systemu operacyjnego (OS).
10. W sklepie App Store wyszukaj aplikację Google Authenticator.
11. Wybierz aplikację mobilną Google Authenticator.
12. Pobierz i zainstaluj aplikację.

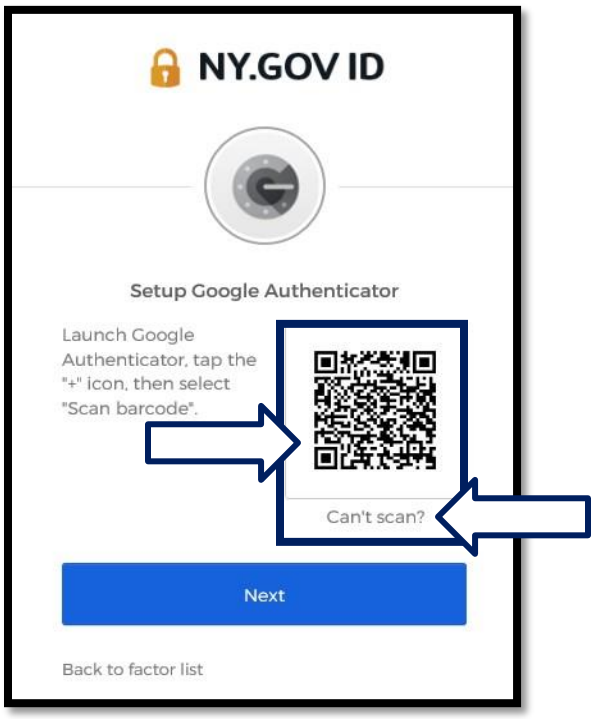


13. Po zainstalowaniu aplikacji Google Authenticator na smartfonie lub tablecie, przejdź do aplikacji na swoim urządzeniu i otwórz ją.

[Kliknij tutaj, aby wrócić do strony głównej]

Otwórz aplikację Google Authenticator na swoim smartfonie lub tablecie.

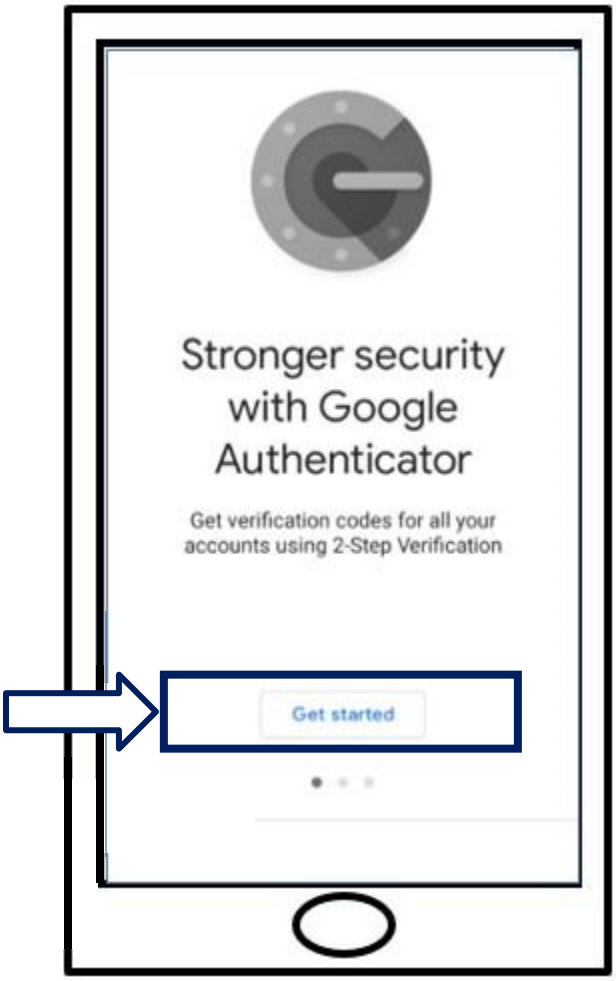
14. Na ekranie komputera pojawi się teraz okno dialogowe z kodem Quick Response (QR).
    - Jeśli nie możesz zeskanować kodu QR, kliknij opcję **Can't Scan?/Nie możesz zeskanować?** pod kodem QR na ekranie komputera. Kliknij tutaj, aby uzyskać instrukcje dotyczące opcji Can't Scan.



15. Przejdź do swojej aplikacji Google Authenticator i otwórz ją.

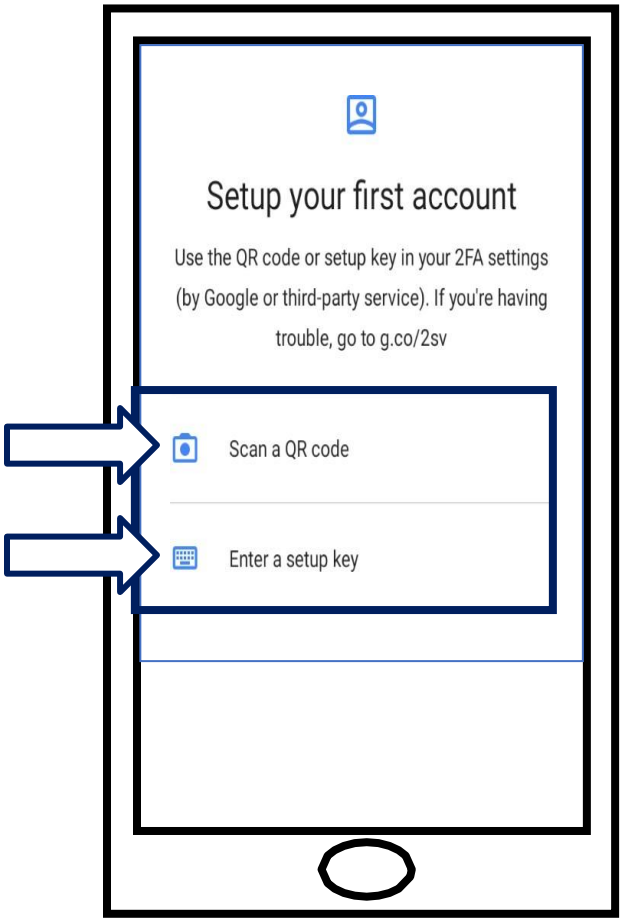
Korzystanie z aplikacji Google Authenticator

16. Na smartfonie zobaczysz ten ekran.



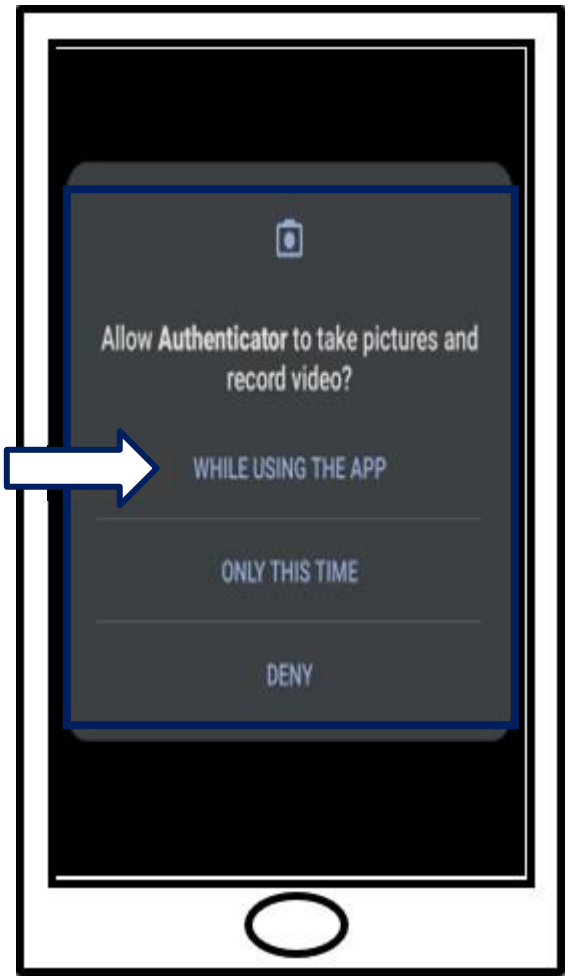
17. Kliknij przycisk **Get Started/Rozpocznij.**

18. Zostanie otwarty ten ekran. Będziesz miał możliwość **zeskanowania kodu QR** lub **wprowadzenia klucza konfiguracji**. Wybierz jedną z tych opcji.



Wskazówki dotyczące używania aplikacji Google Authenticator do skanowania kodu QR: Urządzenie z systemem Android

19. Aplikacja zapyta o zgodę na korzystanie z aparatu. Kliknij przycisk **While Using the App/Podczas używania aplikacji.**



20. Przejdź do skanowania kodu QR.

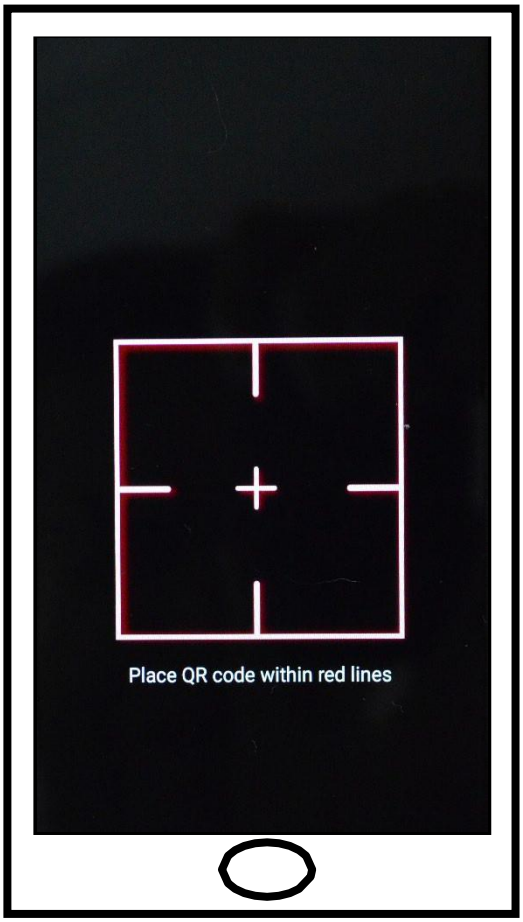
Urządzenie Apple

21. Zobaczysz komunikat, że *aplikacja „Authenticator" chciałaby uzyskać dostęp do aparatu.* Kliknij **OK**.

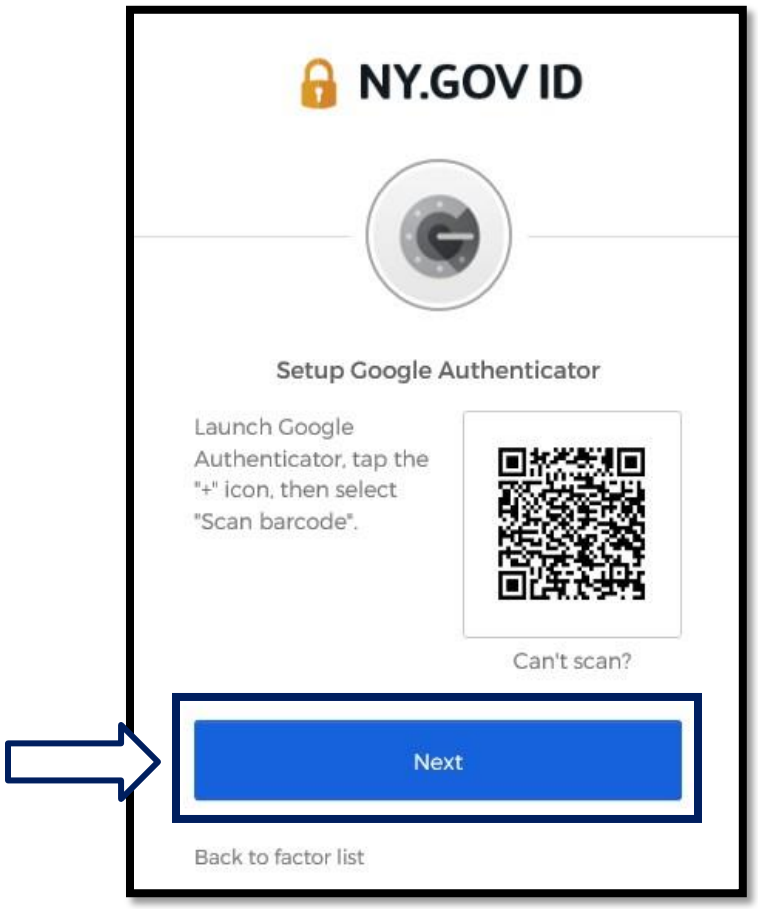
22. Przejdź do skanowania kodu QR.

Zeskanuj kod QR

23. Na ekranie Twojego smartfona pojawi się teraz pusty ekran z kwadratem w środku.



24. Skieruj aparat smartfona lub tabletu na kod QR, który znajduje się na ekranie komputera (patrz poniższy obrazek), tak aby kod QR na ekranie komputera pojawił się w zielonym polu na ekranie smartfona. Aplikacja automatycznie zeskanuje kod do telefonu lub tabletu.



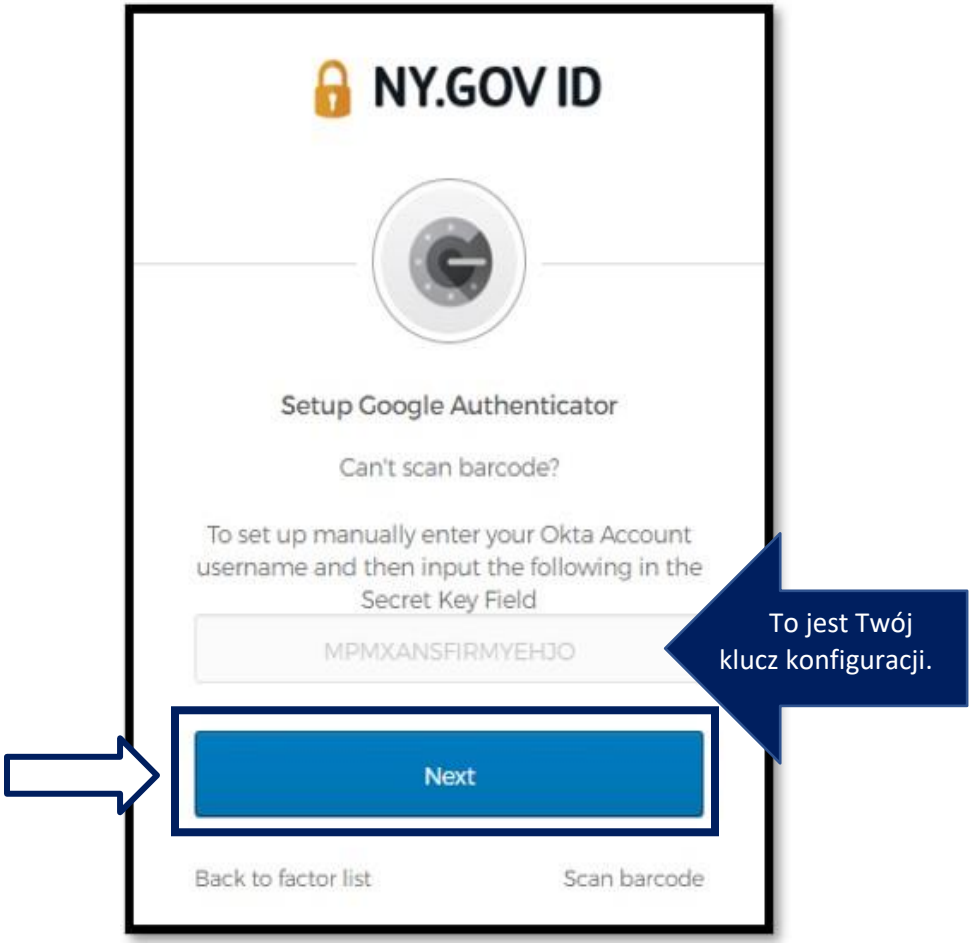
25. Przejdź do wprowadzania kodu krok po kroku.

Wskazówki dotyczące wprowadzania klucza konfiguracji (jeżeli nie możesz zeskanować kodu QR).

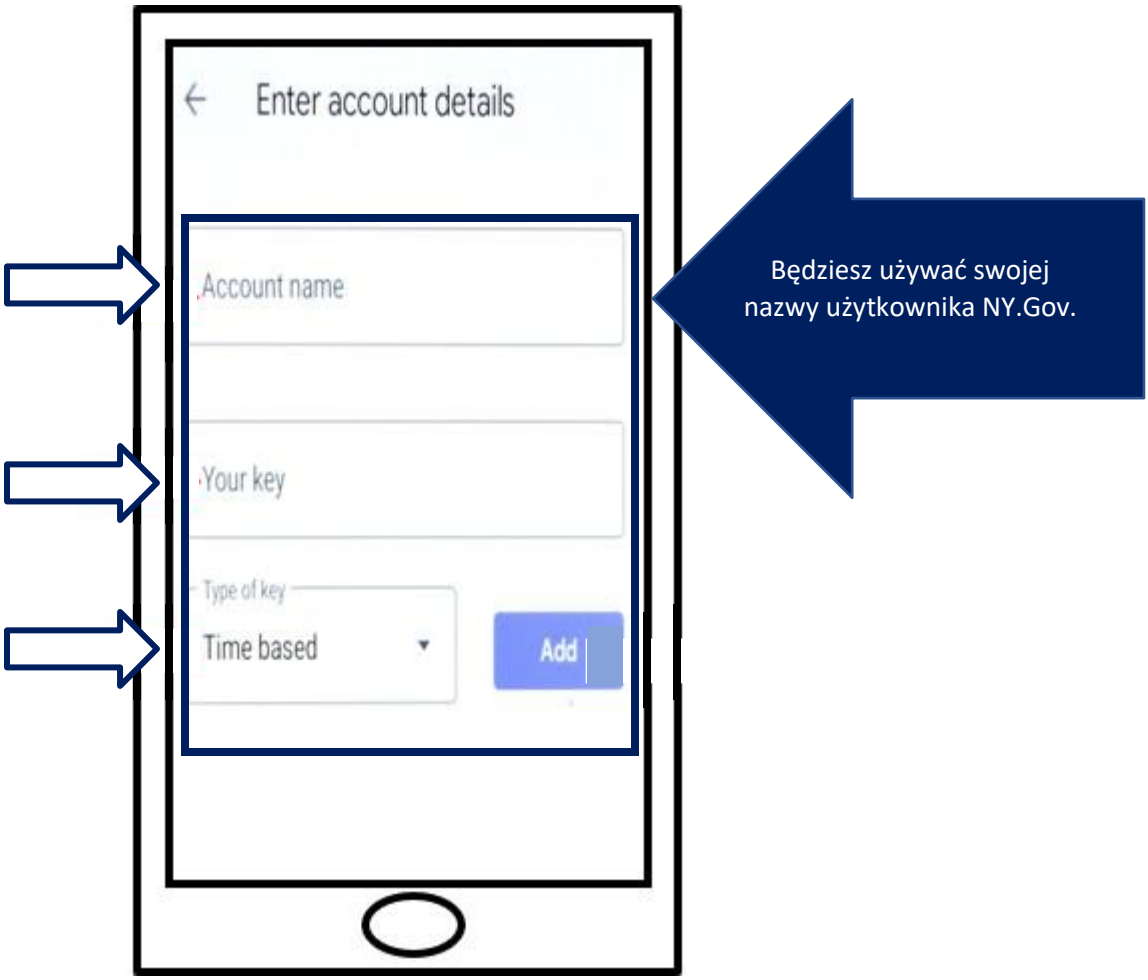
26. Jeśli nie możesz zeskanować kodu, w kroku 13 powyżej wybierz opcję **Enter a setup key/Wprowadź klucz konfiguracji.**

Porada: Kliknij tutaj, aby poznać inne możliwe przyczyny tego błędu oraz sposób ich naprawienia.

27. Na ekranie komputera pojawi się tajny klucz. Jest to kod, który wpiszesz w aplikacji Google Authenticator. Zostanie wyświetlony ekran zawierający instrukcje dotyczące wprowadzania klucza konfiguracji. UWAGA: Aby przejść do tego kroku, musisz najpierw skonfigurować metodę uwierzytelniania wieloczynnikowego Okta Verify.



28. W aplikacji Google Authenticator wprowadź nazwę swojego konta NY.gov, wprowadź swój tajny klucz, wybierz opcję Time based.



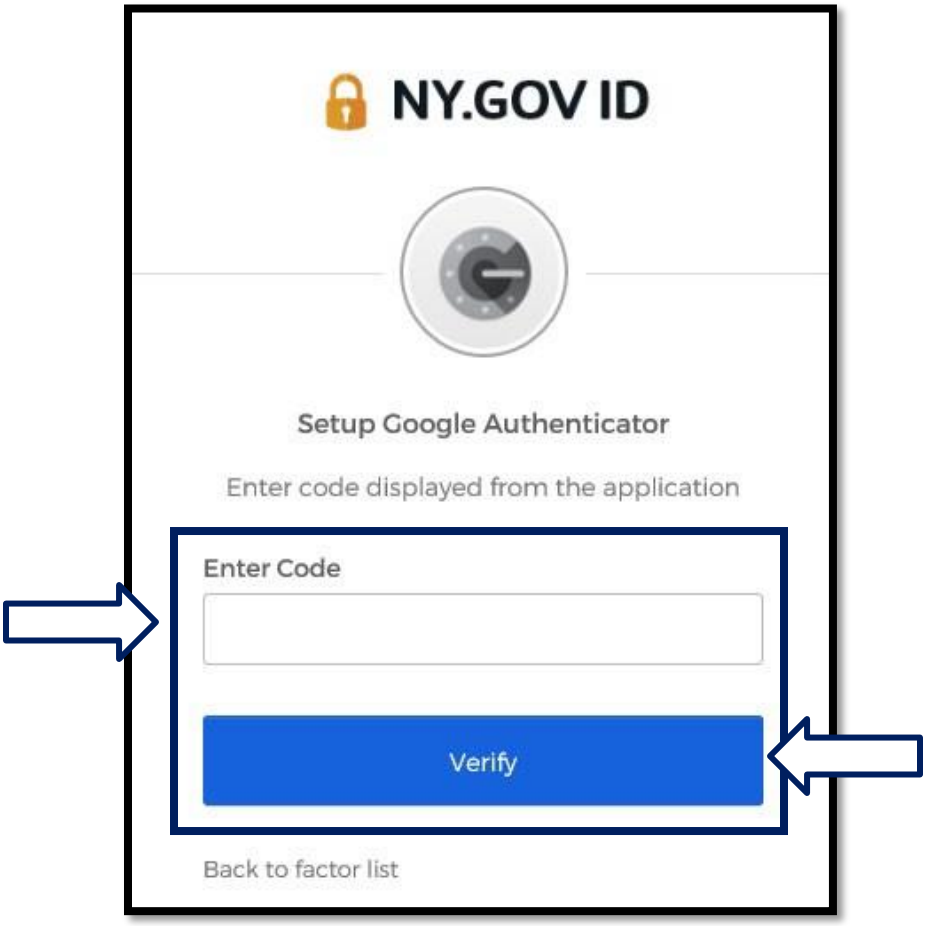
29. Kliknij przycisk **Add/Dodaj.**

30. Przejdź do wprowadzania kodu krok po kroku.

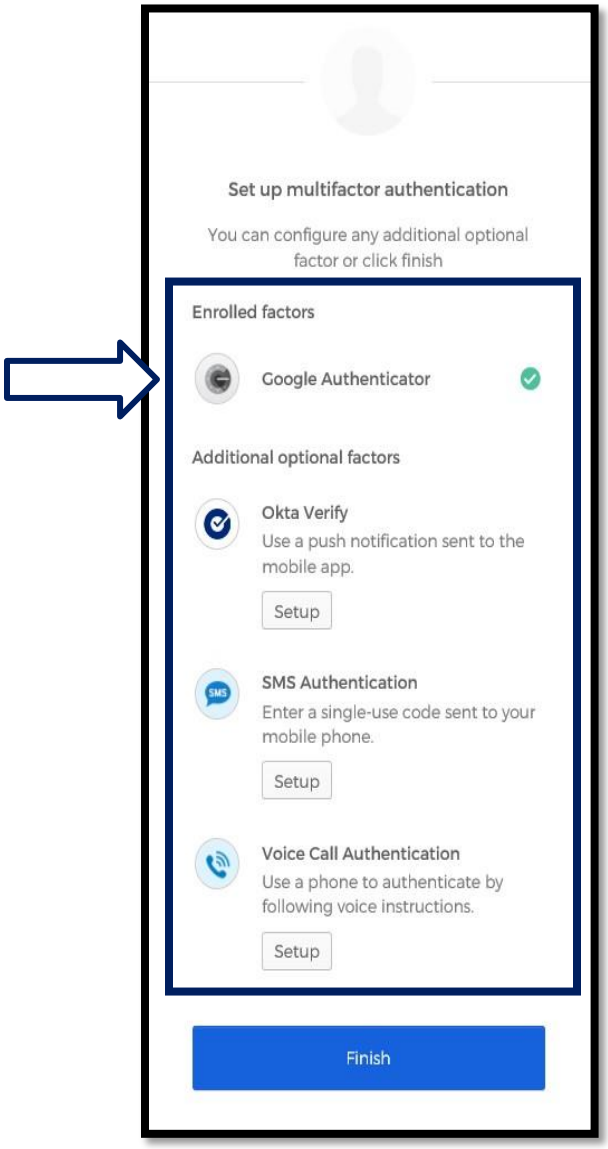
Wprowadzanie kodu

31. Gdy aplikacja pomyślnie zeskanuje kod QR, Twój smartfon wyświetli ekran z Twoją nazwą użytkownika i sześciocyfrowym kodem. Jest to kod, który wpiszesz na komputerze w kolejnych krokach. Kod ten będzie się zmieniał co 30 sekund.

32. Wpisz kod z aplikacji w pole Enter Code/Wpisz kod na monitorze komputera i kliknij **Verify/Zweryfikuj.**



33. Zostaniesz przekierowany z powrotem do ekranu rejestracji, gdzie możesz skonfigurować inną metodę uwierzytelniania wieloczynnikowego. Zwróć uwagę, że Google Authenticator znajduje się teraz pod nagłówkiem Enrolled factors/Zarejestrowane czynniki. Zaleca się skonfigurowanie więcej niż jednej metody uwierzytelniania wieloczynnikowego.

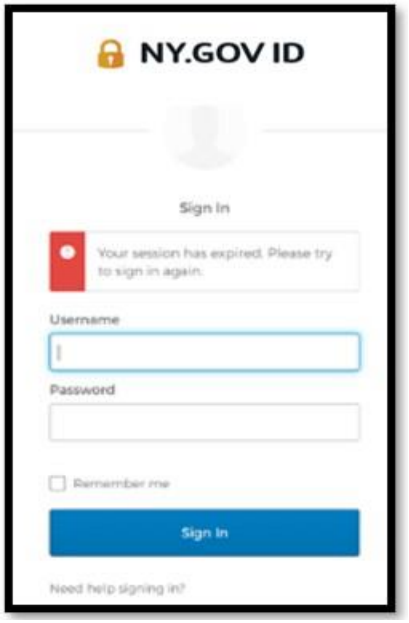


34. Po skonfigurowaniu wszystkich żądanych metod uwierzytelniania wieloczynnikowego kliknij przycisk Finish/Zakończ.

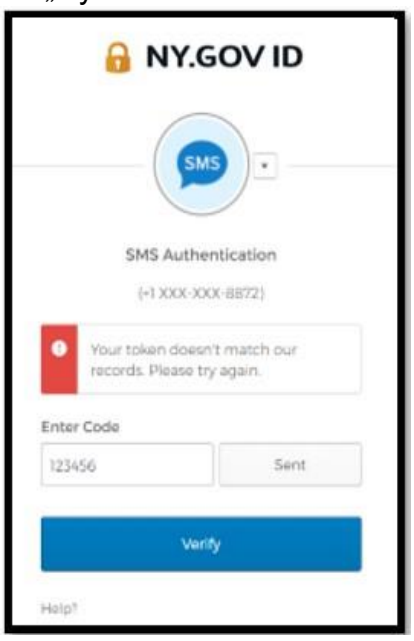
- Porada: Jeśli będziesz konfigurował metodę uwierzytelniania wieloczynnikowego, która wykorzystuje aplikację na telefon, pobierz aplikację przed kliknięciem przycisku Setup/Konfiguruj na stronie przeglądarki „Set up multifactor authentication/Konfiguruj uwierzytelnianie wieloczynnikowe”. Dwie metody uwierzytelniania wieloczynnikowego, które wykorzystują aplikacje, to Okta Verify i Google Authenticator.

Potencjalne komunikaty o błędach i sposoby ich rozwiązywania.

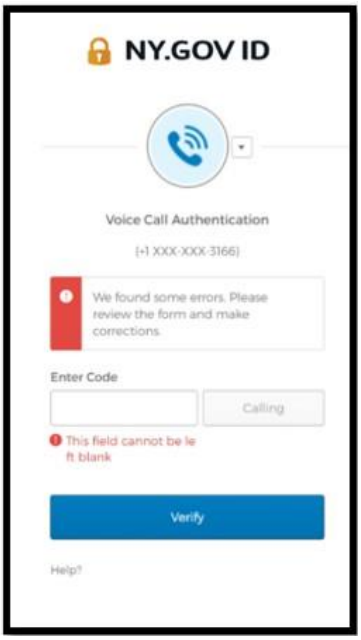
- Komunikat o błędzie: Sesja wygasła.
- Rozwiązanie: Klient musi zalogować się ponownie.



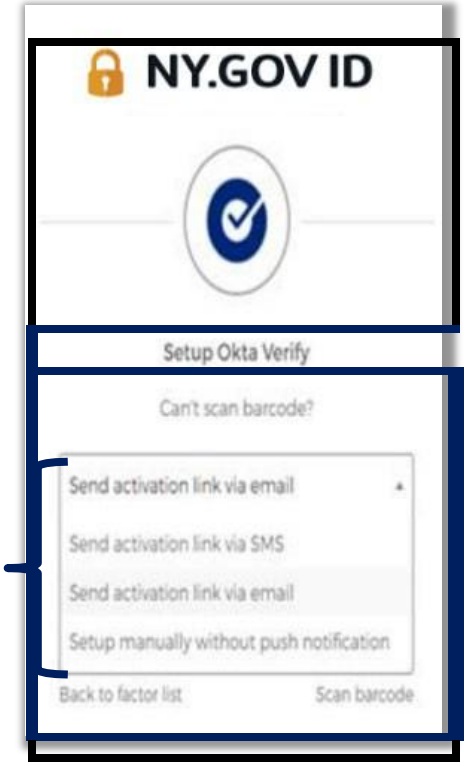
- Komunikat o błędzie: Token nie pasuje.
- Rozwiązanie:
    1. Klient powinien sprawdzić poprawność.
    2. Klient powinien ponownie „wysłać” kod.



- Komunikat o błędzie: Znaleziono błąd.
- Rozwiązanie: Klient musi wprowadzić kod.



- Komunikat o błędzie: Nie można zeskanować kodu kreskowego.
- Rozwiązanie:
    1. Wypróbuj podane metody alternatywne.
        - „Wyślij aktywację SMSem” - klient może wprowadzić numer telefonu.
        - „Konfiguracja ręczna bez push” - klient zobaczy kod tymczasowy.
        - „Wyślij aktywacyjną wiadomość e-mail” - do klienta zostanie wysłana wiadoność e-mail na adres użyty przy tworzeniu konta.



    2. Upewnić się, że urządzenie klienta „zezwoliło” na dostęp do aparatu. (kliknij tutaj, aby uzyskać instrukcje)

Powrót do strony głównej