Highly Regulated Identity

The key to making sensitive customer operations easier and more secure

Organizations across industries have sensitive customer operations that require special user protections when gathering consent. To satisfy end-user expectations, these organizations need to deliver user-friendly digital experiences without falling short of the rigorous security standards their industry requires. Sensitive customer interactions demand an uncompromising balancing act: **security and digital teams must drive robust security and privacy controls along with a seamless UX.**

On both fronts, the stakes are high:

Security and privacy

- **The rising tide of malware, AI, deepfakes, phishing and other increasingly sophisticated social engineering attacks** adds urgency to industry and company-led pushes for enhanced security.
- **Vulnerabilities in end-to-end transaction flows** expose sensitive customer data to unnecessary risk.
- **Complying with industry standards and regulations** intensifies the need for immediate action. In financial services, this is true for regulations such as PSD2 in the EU, the Australian CDR, UK Open Banking, and other Open Banking initiatives globally.

$4.5M The amount that companies lose on average per data breach in 2023, a 15.3% increase from 2020.[1]

Customer experience

- **Frustrating customer experiences lead to abandonment and lower opt-in.** Even with sensitive interactions, users are tired of controls that cause excessive friction like MFA bombing.
- **Great customer experiences begin with a high level of trust.** Without confidence in your organization's security and privacy measures, consumers (especially younger generations) will likely choose a brand that emphasizes trust — and delivers a more secure customer experience.

60% of consumers have purchased something from one brand over another based on the service they expect to receive.[2]

58% of Millennials and Gen Zers won't even touch a digital service until they've confirmed the organization has a solid reputation for safeguarding data.[3]

For sensitive customer operations, organizations need an Identity-powered security solution that minimizes the risk of threat actors, supports regulatory requirements and enables superior digital experiences. Without it, they risk fraud, data breaches, low levels of customer trust, and threats to core business and growth strategies.

In this datasheet:

- Examples of sensitive customer operations across industries
- How the Okta Highly Regulated Identity Solution Suite helps

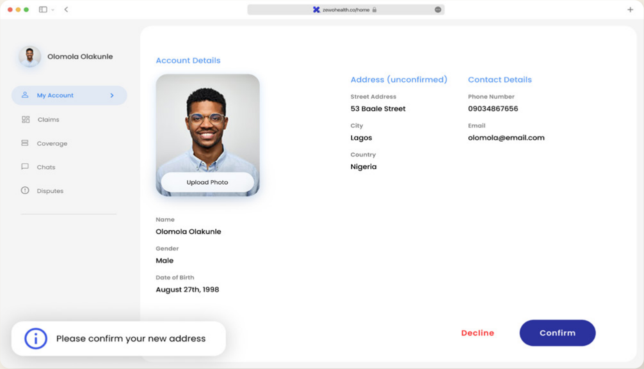
[1] Cost of a Data Breach Report, IBM, 2023 [2] CX Trends Report, Zendesk, 2023 [3] Why Digital Trust Matters Report, McKinsey, 2022

Building better customer experiences — securely

Leaders in highly regulated industries need a solution that prioritizes security and UX equally. By applying a solution that is built for both powerful security and seamless UX, organizations resolve the common issues that arise when these two areas come into conflict. Let's look at some examples of sensitive operations:

Example: Identity verification for account changes

For common sensitive operations like changing account information, admin or security settings or accessing sensitive data, step-up security and get user consent with the following steps:



Account Details

Address (unconfirmed)

Street Address
53 Baale Street

City
Lagos

Country
Nigeria

Contact Details

Phone Number
09034867656

Email
olomola@email.com

Name
Olomola Olakunle

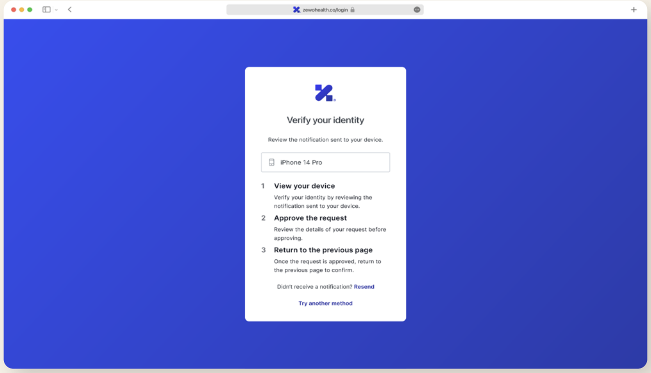
Gender
Male

Date of Birth
August 27th, 1998

Please confirm your new address

Step 1: Initiate

User would like to initiate an address change within their account profile.



Verify your identity

Review the notification sent to your device.

1 View your device
Verify your identity by reviewing the notification sent to your device.

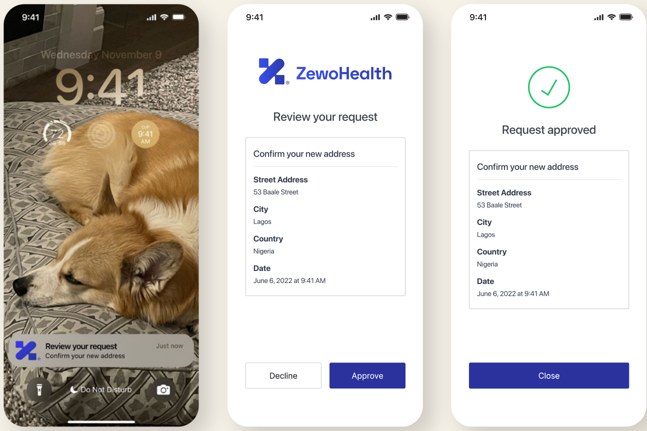
2 Approve the request
Review the details of your request before approving.

3 Return to the previous page
Once the request is approved, return to the previous page to confirm.

Didn't receive a notification? Resend

Step 2: Verify Identity

This request prompts an additional security measure. The user is prompted for a second Identity factor, such as push notification to mobile, WebAuthn, OTP (generated on mobile), or OTP sent over SMS.



Review your request
Confirm your new address

Review your request

Confirm your new address

Street Address
53 Baale Street

City
Lagos

Country
Nigeria

Date
June 6, 2022 at 9:41 AM

Request approved

Confirm your new address

Street Address
53 Baale Street

City
Lagos

Country
Nigeria

Date
June 6, 2022 at 9:41 AM

Step 3: Approve change

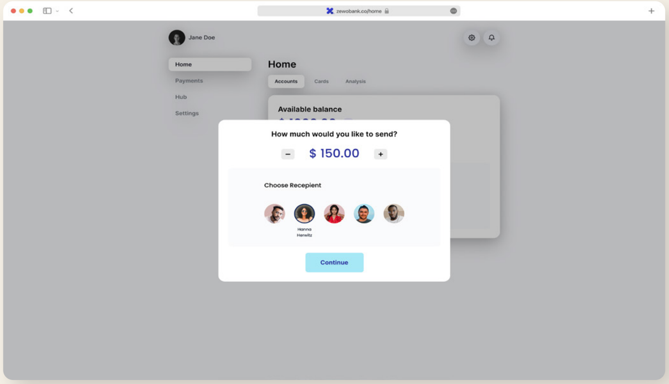
Once the user has verified their identity, they review the address change details and approve the new address request.

Example: Identity verification for a money transfer

For common sensitive financial operations like money transfers or payments, step-up security and get user approval with the following steps:

Step 1: Initiate transfer

User would like to initiate a money transfer directly from their bank.



zewobank.co/home

Jane Doe

Home
Payments
Hub
Settings

Home

Accounts Cards Analysis

Available balance

How much would you like to send?

– $ 150.00 +

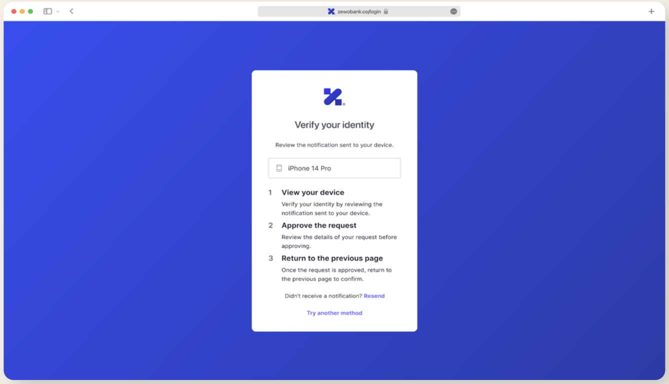
Choose Recepient

Hanna Herwitz

Continue

Step 2: Verify Identity

This request prompts an additional security measure. The user is prompted for a second Identity factors, such as push notification to mobile, WebAuthn, OTP (generated on mobile), or OTP sent over SMS.



zewobank.co/login

Verify your identity

Review the notification sent to your device.

iPhone 14 Pro

1 **View your device**
Verify your identity by reviewing the notification sent to your device.

2 **Approve the request**
Review the details of your request before approving.

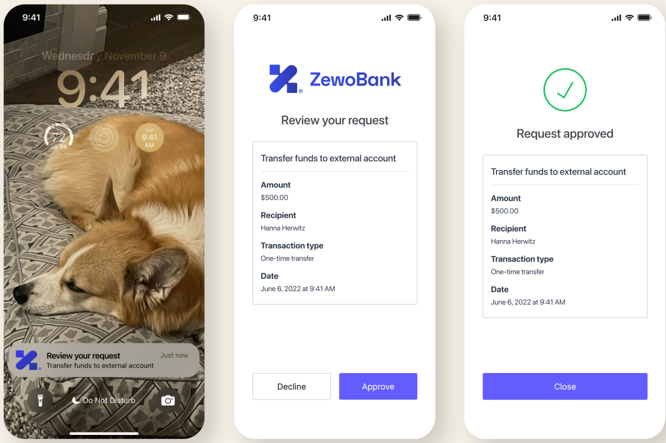
3 **Return to the previous page**
Once the request is approved, return to the previous page to confirm.

Didn't receive a notification? Resend

Try another method

Step 3: Approve transaction

Once the user has completed the verification, they confirm specific chosen transaction details, approve payment and complete the transaction.



9:41

Wednesday November 9

9:41

Review your request Just now
Transfer funds to external account

Do Not Disturb

9:41

ZewoBank

Review your request

Transfer funds to external account

Amount
$500.00

Recipient
Hanna Herwitz

Transaction type
One-time transfer

Date
June 6, 2022 at 9:41 AM

Decline Approve

9:41

Request approved

Transfer funds to external account

Amount
$500.00

Recipient
Hanna Herwitz

Transaction type
One-time transfer

Date
June 6, 2022 at 9:41 AM

Close

Sensitive customer operations across industries:

Finance

- Sending money to any person with any provider
- Changing payee details on recurring payments
- Open banking payments that conform with evolving regional regulatory standards
- Verifying a customer's Identity at a point-of-sale terminal or banking branch
- Verifying a user's Identity during a call center interaction
- Securing a customer's consent to share Personally Identifiable Information (PII)

Healthcare

- Accessing personal health information or test results in a portal
- Providing consent to share personal health information with a provider
- Paying a healthcare provider

Retail

- Processing returns and refunds (while reducing fraudulent claims)
- Changing profile information (address, email, phone number)
- Accessing loyalty programs and redeeming points

Transportation/Logistics

- Enacting a change of address on a high-value package
- Accessing a request portal for fleet requests
- Authorizing changes to delivery schedules/routes

Manufacturing

- Granting access to suppliers or vendors
- Approving/rejecting products based on quality standards

Bottom line:

Trust is essential to driving the adoption of digital services and reducing fraud. To meet the elevated user experience and security requirements for sensitive customer scenarios, organizations need user-friendly ways to build a high level of trust and ensure the operation is secure end to end.

Datasheet April 2024

Okta Highly Regulated Identity

For sensitive customer operations

Okta Highly Regulated Identity brings authentication and authorization of consumer transactions and other operations to the financial grade level of assurance. As part of our best-in-class Customer Identity Cloud, Okta Highly Regulated Identity delivers user-friendly Financial Grade Identity™ measures that support better user experiences and build trust into the foundations of your digital offerings.

Highly Regulated Identity helps answer three questions:

1. Is the user who they say they are?

Strong Customer Authentication (SCA) is an authorization framework that began in Financial Services. It ensures the secure execution of sensitive digital interactions by leveraging dynamic, context-specific MFA.

2. Did the user give informed consent to the transaction?

Dynamic Linking ties transaction details to the SCA approval confirmation to help prevent transaction tampering.

Rich Authorization Requests communicate this contextual information to the user as part of the SCA approval request. For example, once a user's identity is verified, a banking SCA push approval may ask: "Do you approve a person to person payment to John Smith for $1,000?”

3. Is the approval process secure end-to-end?

OpenID FAPI 1 Advanced Protocols elevate data privacy and app security for the end-to-end flow. Okta employs a number of features to help you adhere to this rigorous authorization framework:

- **JAR (JWT-Secured Authorization Requests) –** Protects the integrity of authorization request parameters with non-repudiation via message-level signing of the authentication request.
- **PAR (Pushed Authorization Requests) –** Allows requests to be routed via the backchannel and away from the browser.
- **Private Key JWT –** Strong app authentication using cryptographic keys.
- **mTLS (OAuth 2.0 Mutual-TLS Client Auth and Certificate-Bound Access Tokens) –** Use PKI for strong app authentication and/or certificate-bound access tokens.
- **JSON Web Encryption –** Locks down sensitive data in encrypted tokens.

Why Okta

Partner with the leader in Identity

Okta is the world's leading born-in-the-cloud Identity partner, offering an always-on private or public cloud solution with a global cell infrastructure capable of handling billions of transactions per day.

Deliver intuitive user experiences

Okta CIC integrates easily with existing cyber infrastructure, enabling your organization to implement CX improvements faster and send enriched approval requests only when necessary.

Drive agility and reduce costs

Ease cost pressures with a scalable, reliable, and extensible Identity solution that bolsters security and substantially reduces your risk level — without sacrificing agility.

Increase security and prevent fraud

Fight sophisticated cyber threats with high assurance security measures like SCA and FAPI protocols, that help to prevent fraud.

Stay compliant, confidently

By providing a certified FAPI 1 Advanced security profile, Okta Highly Regulated Identity lays the groundwork for processes that comply with FDX in the US, PSD2 in the EU, CDR in Australia, and various open banking requirements.

Ready to see it in action?

Connect with our team and schedule your free demo.
okta.com/webinars/hub/?type=demo

These materials and any recommendations within are not legal, privacy, security, compliance, or business advice. These materials are intended for general informational purposes only and may not reflect the most current security, privacy, and legal developments nor all relevant issues. You are responsible for obtaining legal, security, privacy, compliance, or business advice from your own lawyer or other professional advisor and should not rely on the recommendations herein. Okta is not liable to you for any loss or damages that may result from your implementation of any recommendations in these materials. Okta makes no representations, warranties, or other assurances regarding the content of these materials. Information regarding Okta's contractual assurances to its customers can be found at okta.com/agreements. Any products, features or functionality referenced in this material that are not currently generally available may not be delivered on time or at all. Product roadmaps do not represent a commitment, obligation or promise to deliver any product, feature or functionality, and you should not rely on them to make your purchase decisions.