YEO CFR SDK

IN APPLICATION SECURITY WHITEPAPER

The Session Gap After Login

How continuous identity assurance helps banks protect high-risk digital journeys



September 2026
© 2026 YEO messaging Ltd
Registered in England and Wales 10785061

Contents

3 Executive summary

4 The session-level identity gap after login

8 The case for continuous identity assurance

14 Reducing unnecessary step-up code friction

17 App reimbursement and session-level risk

20 Privacy and data architecture

22 Where CFR fits in the banking journey

25 A practical evaluation framework

27 Conclusion





Executive Summary

Banks have invested heavily in KYC, customer onboarding and strong authentication to establish who a customer is and decide whether access should be granted. Most of that investment is concentrated at enrolment and login — including native device biometrics such as Face ID, which strengthen that moment but are controlled by the device, not the bank, and end the instant the session begins.

That leaves far less assurance about who remains in control once an authenticated session is active. A valid login does not prevent account takeover, session hijacking, unattended-device use or another person operating a trusted session.

continues to match the enrolled customer, using facial matching, liveness detection and supported depth signals processed on the user's device.

YEO's Continuous Facial Recognition SDK adds an identity-assurance signal during the session itself. It helps the bank verify that the person present

Three Outcomes

1. Stronger bank-configured session assurance

Banks can introduce an additional identity signal after login and during sensitive activity.

2. More informed fraud decisions

CFR can identify absence, mismatch or failed-liveness events within an authenticated journey and feed those signals into the bank's existing risk controls.

3. Less unnecessary interruption

Where architecture, policy and regulation allow, passive assurance can reduce dependence on repeated customer challenges.

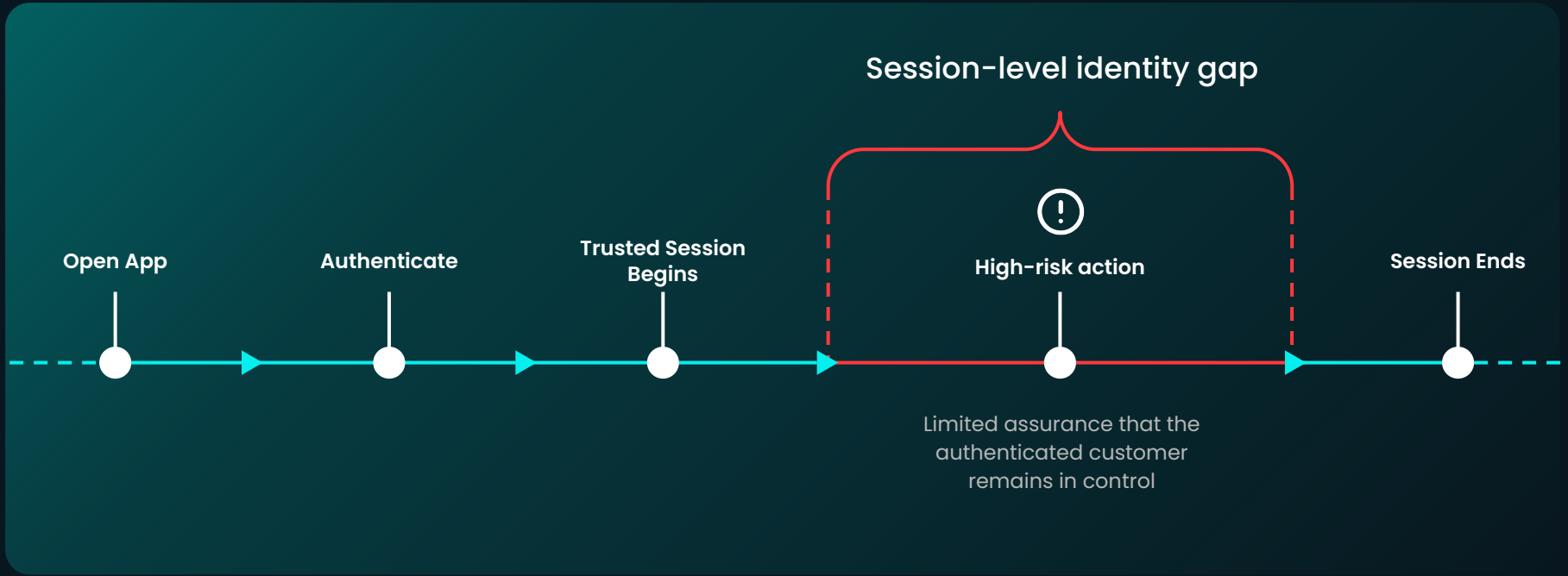
Key Takeaway

KYC establishes identity. Authentication grants access. Continuous identity assurance helps the bank maintain confidence after login.

The session-level identity gap after login

Digital banking security often treats authentication as the point at which identity has been established. The customer provides a password, passkey, biometric, device signal or one-time code. The bank evaluates the evidence, grants access and creates a trusted session.

The control is essential, but the identity of the person operating the session can change after access has been granted.



The most consequential risks frequently occur after authentication

- A customer leaves an unlocked device during an active banking session.
- A fraudster obtains valid credentials and completes a point-in-time challenge.
- Malware, remote-access software or compromised session data gives another person control after login.
- A one-time code is intercepted, phished or approved under social engineering.
- A person other than the enrolled customer operates a shared or delegated device.

In each case, the bank may have evidence that the account was authenticated without evidence that the account holder remained in control when a beneficiary was changed, a payment was approved or sensitive information was accessed.

This is the session-level identity gap.

The difference in one view

The point is not to remove layered authentication. It is to make the layer model complete.

Point-in-time authentication	YEO's continuous identity assurance
Confirms a factor at a specific moment	Confirms whether the enrolled person remains present
Concentrated at login or selected step-up points	Extends identity assurance into active sessions and high-risk activity
May rely on credentials, possession or a one-off biometric	Adds on-device facial matching, liveness and supported depth signals
Produces an access or step-up decision	Produces a session-level identity signal for bank policy and audit

Different controls answer different questions

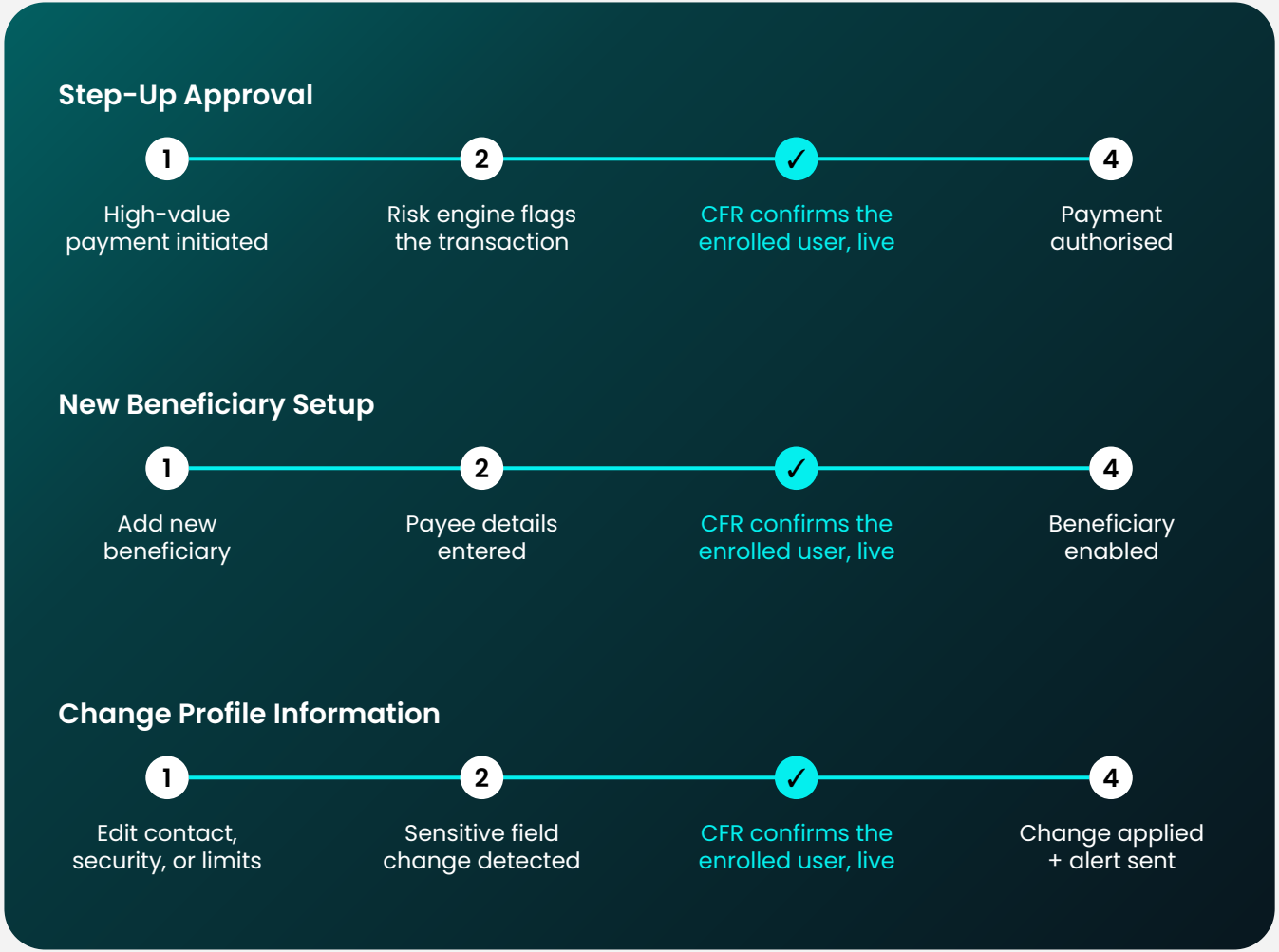
Continuous identity assurance does not replace a bank's existing fraud and authentication controls. It addresses a distinct identity question within a layered security model.

These controls are complementary rather than interchangeable. Device, behavioural and transaction signals assess risk. CFR adds evidence about the identity and presence of the person operating the session.

Control layer	What it helps the bank understand	What it may not establish on its own
Device and network intelligence	Whether the device, connection, IP address or digital identity has previously been associated with suspicious activity.	Whether the person physically present is the enrolled customer.
Behavioural biometrics	Whether navigation, typing, touch, cursor movement or hesitation differs from an established behavioural pattern.	The physical identity of the person operating the session. Confidence may also depend on the availability of a reliable behavioural baseline.
Transaction monitoring	Whether a payment or account action appears unusual in value, destination, timing or context.	Whether the enrolled customer is present when the action is completed.
YEO CFR	Whether the person present continues to match the enrolled customer during selected points in the session.	Network-wide fraud patterns, device reputation, mule activity, transaction anomalies or customer intent. Existing controls remain necessary.

How CFR fits your payment workflows

Three moments in the mobile payment journey where fraud risk peaks — and where continuous, on-device verification steps in.



Every checkpoint runs on-device, in real time — no redirect, no extra app, no added friction for the genuine user.

The case for continuous identity assurance

Stronger session controls, clearer evidence and fewer unnecessary interruptions



1. Regulatory relevance: stronger controls, clearer evidence

Banking regulation does not prescribe one universal identity technology. It does expect firms to understand their risks, apply proportionate controls and demonstrate how those controls perform.

In the UK, the FCA's Consumer Duty [2] requires firms to act in good faith, avoid foreseeable harm and support customers in pursuing their financial objectives. The APP scam reimbursement requirement also increases the commercial importance of preventing avoidable fraud.

In the United States, FFIEC [3] guidance emphasises risk assessments, layered security and stronger controls for higher-risk transactions and activities.

Across the Middle East, regulators are also strengthening expectations around digital security, technology risk and consumer protection.

The Central Bank of the UAE's Consumer Protection Standards address the protection of consumer information and the security of digital financial services.[4] In Saudi Arabia, the Saudi Central Bank's Cyber Security Framework requires regulated institutions to identify and manage cyber risks through effective governance and controls.[5]

At an international level, FATF guidance encourages financial institutions to take a risk-based approach to digital identity and to consider identity assurance in customer due diligence, authentication and ongoing monitoring.[6]

YEO CFR does not make a bank compliant. It gives the bank an additional, testable session control that can support its wider fraud, customer-protection and operational-resilience framework.

What YEO's CFR can help a bank demonstrate

- Identity controls that extend beyond onboarding and login.
- A risk based control for sensitive activity within an authenticated session.
- A privacy-conscious approach that does not require a central YEO biometric database.
- A configurable response to absence, mismatch or failed liveness.
- Session-level event data to support review, investigation and governance.

Global relevance, local implementation

Important: Each institution must validate the regulatory mapping for its jurisdiction, products and customer journeys. CFR can support a compliance strategy, but it does not replace legal, risk or regulatory analysis.

Market	Banking consideration	Potential CFR role
United Kingdom	Consumer Duty, APP reimbursement and payment-services obligations [7]	Adds a preventative session signal and evidence for control design
United States	Risk-based authentication and layered-security expectations	Adds identity evidence that can be applied to higher-risk activity
UAE and Gulf markets	Strong authentication, digital fraud and technology-risk expectations	Adds session-level liveness and identity assurance alongside KYC and authentication
South Africa	Cyber resilience and data-minimisation requirements	On-device processing can support a privacy-conscious deployment model
Canada and other markets	Evolving privacy, digital identity and fraud-management expectations	Adds identity assurance without requiring YEO to hold a central biometric database

2. Fraud: the risk begins after authentication

CFR addresses a specific question: does the person controlling an authenticated session continue to match the enrolled customer?

It should be evaluated against that defined role, rather than positioned as a complete fraud-prevention system.

Attack coverage: an honest view

Attack pattern	How CFR helps	Coverage
Post-login session takeover	Compares the person present with the enrolled identity during the session	Direct
Unattended-device use	Detects absence and allows the bank to pause, restrict or step up the journey	Direct
Photo or video replay	Uses liveness and supported depth signals to detect common presentation attacks	Direct
Credential-only account takeover	Adds facial identity evidence beyond possession of credentials or a device	Direct
OTP interception or SIM swap	Can reduce reliance on repeated codes in selected journeys	Supporting
Synthetic media or feed injection	Adds another signal but must sit alongside device and application-security controls	Supporting
Coached or authorised APP fraud	The genuine customer may be present while acting under manipulation	Not a direct control

A policy response, not simply an alert

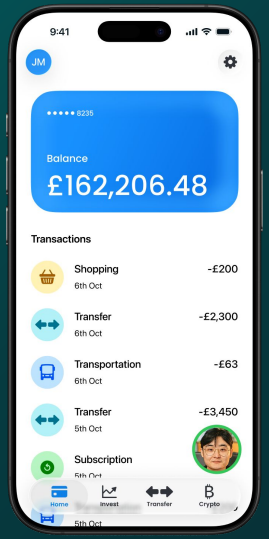
When CFR detects absence, mismatch, failed liveness or a drop in confidence, the bank decides how the journey should respond according to the action and level of risk.

Example Responses:

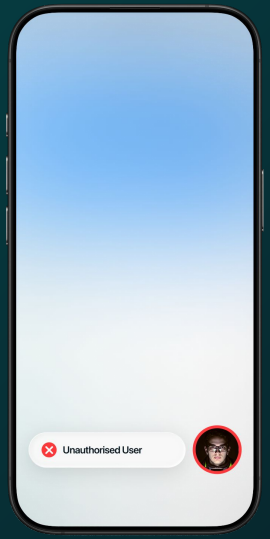
- Allow the session to continue when confidence remains above the approved threshold.
- Request re-verification or another step-up control when confidence declines.
- Restrict a beneficiary change, payment approval or account-setting change.
- Send the event to fraud operations or the bank's decisioning engine.
- Pause or terminate the session when the bank's minimum threshold is not met.

The SDK becomes part of the bank's decisioning architecture rather than a standalone biometric feature.

Confidence Configuration Example



Confidence above threshold: session continues



Confidence degraded: Confidence reduced: bank-defined warning, reverification or restriction



Confidence below minimum threshold: Confidence below minimum: bank-defined pause or termination

The financial case is measurable

The value of continuous identity assurance is not limited to fraud prevention. It can also be measured through the cost of authentication challenges, customer-support demand, abandoned journeys and operational investigations.

The examples (right) illustrate the scale of the opportunity. They are not claimed YEO savings. Actual benefits must be validated using the bank's own volumes, costs, risk policies and pilot results.

A YEO pilot should establish the current baseline, deploy CFR in one defined journey and measure the difference in fraud signals, challenges, support contacts, completion and customer friction.

Authentication cost

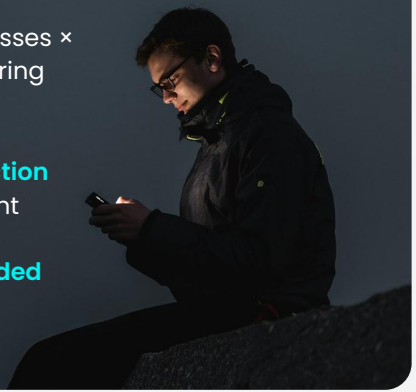
Avoidable challenges removed × fully loaded cost per challenge.



Fraud-loss reduction

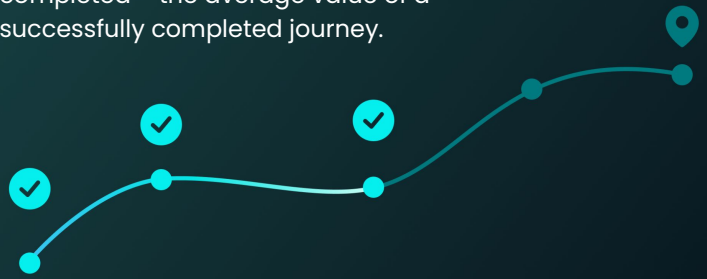
Relevant post-login fraud losses × reduction demonstrated during controlled testing.

For example, every **1% reduction** against a **£10 million** relevant annual fraud-loss baseline represents **£100,000 in avoided loss**.



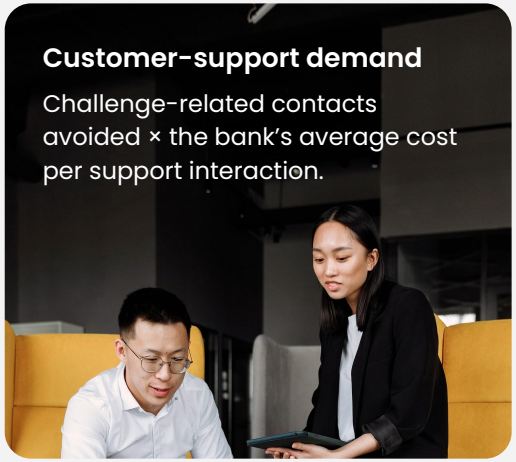
Journey completion

Additional legitimate journeys completed × the average value of a successfully completed journey.



Customer-support demand

Challenge-related contacts avoided × the bank's average cost per support interaction.



Reducing unnecessary step-up code friction

Maintaining identity assurance without repeatedly interrupting legitimate customers

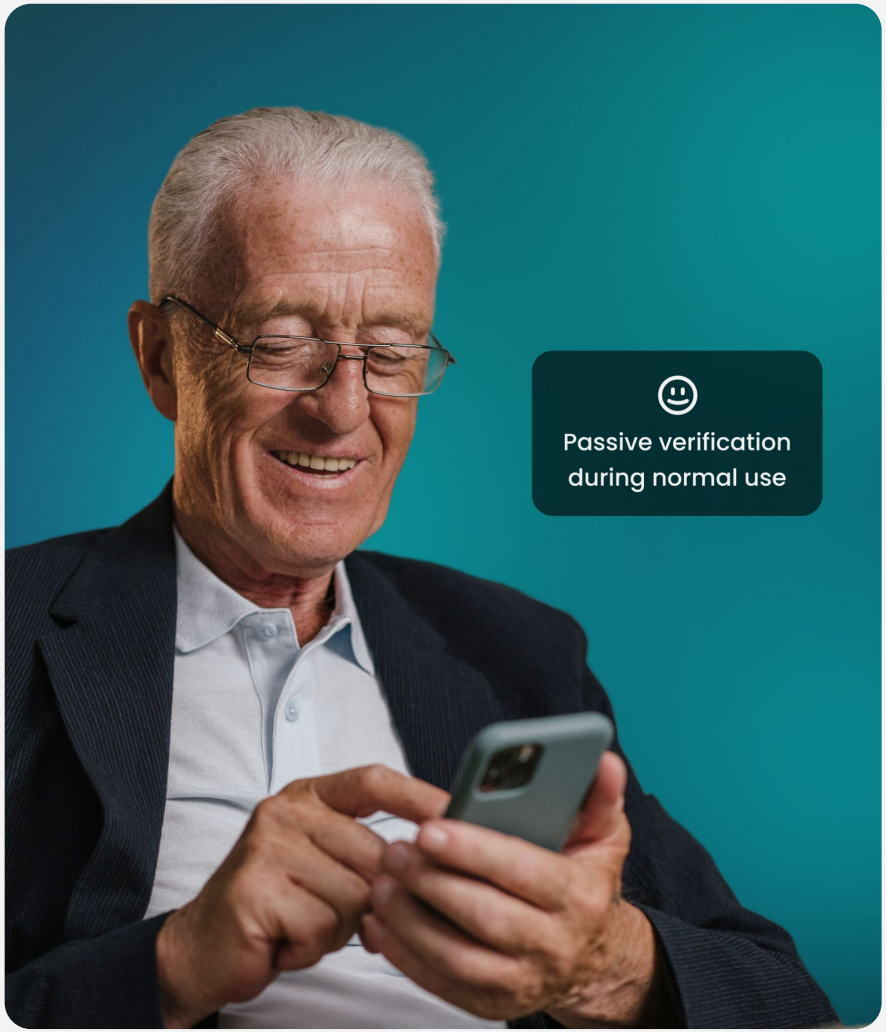


Step-up codes: A cost, friction, and attack-surface question

One-time codes remain an important control in many banking journeys. They may arrive by SMS or be generated inside the banking app. Both approaches require the customer to stop, retrieve or approve a code and then return to the journey.

SMS delivery also introduces telephony cost and channel-specific risks, including interception, delay, social engineering and SIM-swap attacks. In-app codes remove the SMS channel but still depend on the device being in the right hands.

Continuous identity assurance offers another option within an active session. Where policy and regulation allow, the bank can use passive on-device verification instead of repeating a possession-based challenge at every sensitive moment.



Traditional step-up model vs. CFR-enabled assurance

The right deployment is not “remove step-up codes everywhere.” It is to identify where repeated step-up challenges — SMS or in-app — add cost and friction without giving a bank confidence in who is actually operating the session.

→ Building a bank-specific case

The financial case should be calculated using the bank’s own data.

→ Potential annual step-up cost baseline

Number of SMS-delivered codes per year × fully loaded cost per successful and failed delivery, plus the support cost of in-app code journeys

→ Potential customer-friction baseline

Step-up-triggered abandonment rate × average journey value or service cost

→ Potential fraud exposure baseline

Post-login takeover losses + investigation cost + remediation cost + relevant reimbursement exposure

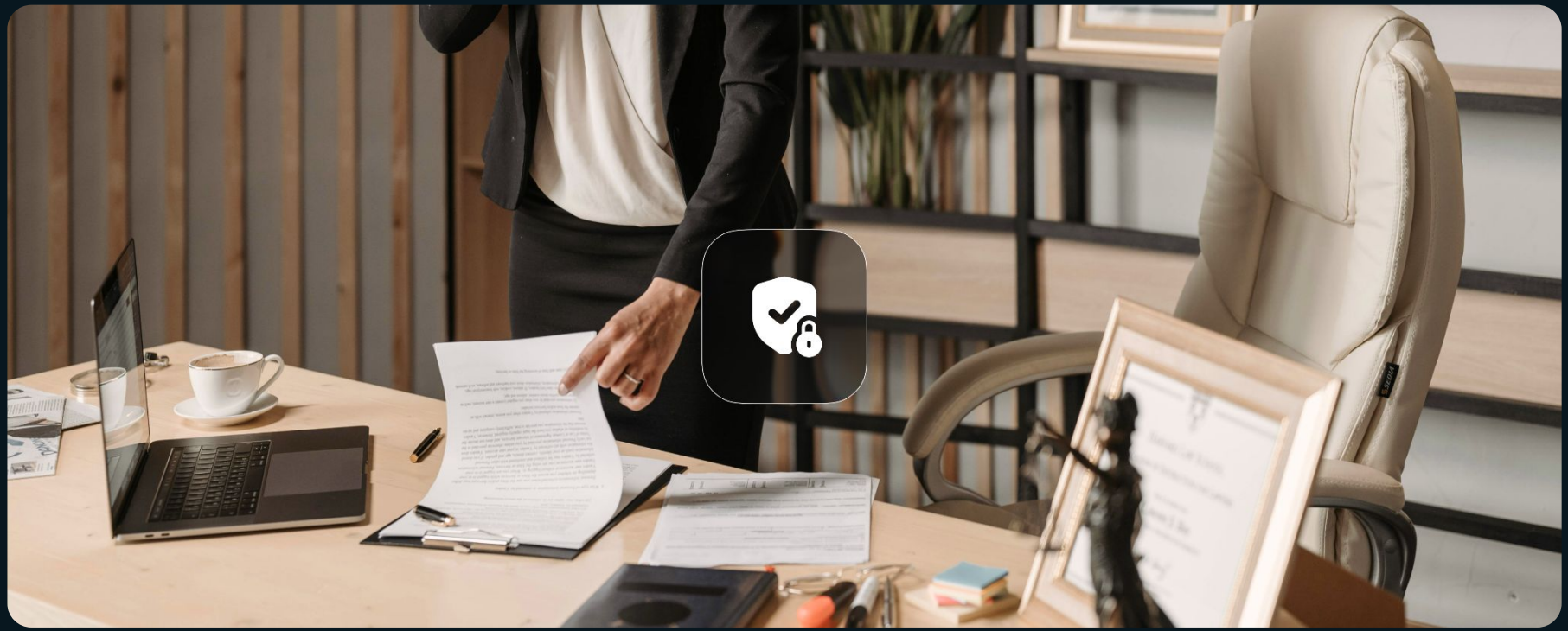
→ Potential CFR benefit

The value of specific step-up journeys safely redesigned, plus losses and operating effort avoided where continuous verification prevents or contains a session takeover.

Traditional Step-Up	YEO’s CFR-enabled approach
Step-up baseline: annual challenge volumes, delivery cost, failure rates and support demand.	Can run passively on the device during approved journeys.
Asks the customer to retrieve or approve a code	Uses the enrolled person's presence as an additional identity signal
SMS codes introduce delivery cost and channel-specific risk	Does not depend on an SMS or in-app code-delivery channel
Strong login, followed by assumed user presence	Identity can be reassessed during the session or before a sensitive action

APP reimbursement and session-level risk

Separating customer manipulation from unauthorised control of a trusted session



APP reimbursement raises the cost of weak session controls

The UK's APP scam reimbursement requirement took effect on 7 October 2024. For eligible Faster Payments claims, the maximum reimbursement level is £85,000.[1] PSR reporting states that £316 million was reimbursed during the first 18 months of the policy.

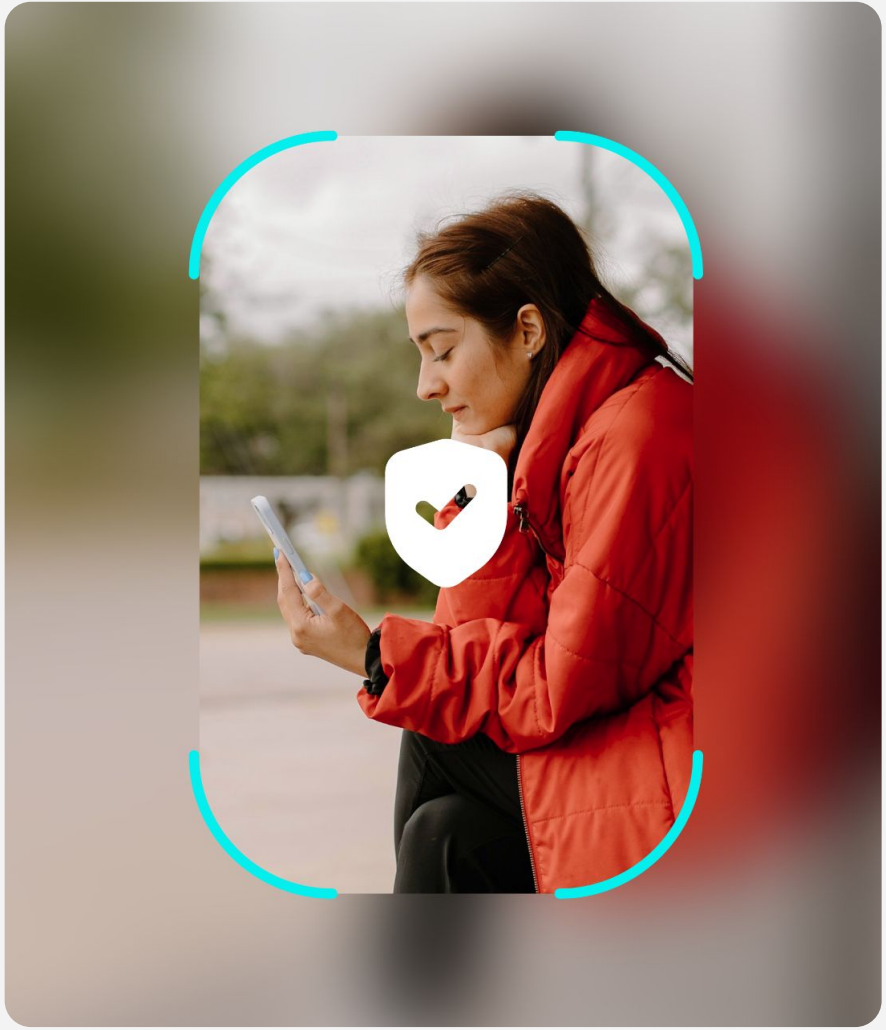
CFR does not identify every APP scam. A genuine customer may be present while acting under manipulation. Behavioural, payment-risk and customer-protection controls remain essential in those cases.

CFR is directly relevant when an unauthorised person takes control after the account has been legitimately authenticated. It can also provide session-level evidence for investigation and decision review.

For banks, the practical question is not whether CFR can solve every APP scam. It is whether their current control stack can distinguish:

1. **Verified customer present and acting under manipulation: CFR is not a direct control.**
2. **Another person operating the customer's trusted session: CFR provides a direct identity signal.**

Where it cannot, CFR adds a new evidential control point.



The control questions CFR adds

Section 6 showed how CFR complements the controls you already run. Here's what that adds specifically to your audit trail and decision record — the questions fraud operations, complaints teams and Consumer Duty governance can now answer that they couldn't before.

This is an important distinction for fraud operations, complaints teams, Consumer Duty governance and payment-risk owners.

Existing control question	Additional CFR question
Did the customer authenticate?	Did the enrolled customer remain present during the activity?
Was the payment challenge completed?	Was the verified person present when the challenge was completed?
Did behavioural or transaction monitoring identify risk?	Did an absence, mismatch or liveness event occur before the action?
Can the bank explain its decision?	Can the bank include session-level identity evidence in its decision record?

Privacy and data architecture

How YEO minimises the biometric data that needs to leave the customer's device



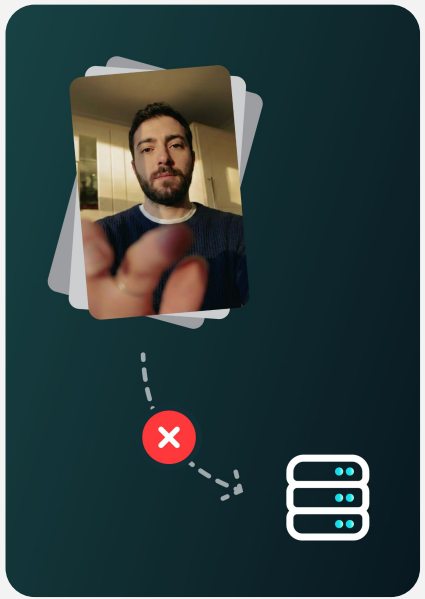
On-device processing and bank-controlled governance

Facial matching, liveness analysis and supported depth verification take place on the user's device. YEO does not require a central YEO store of facial images or biometric templates to perform session verification.

The architecture reduces the amount of sensitive biometric data that needs to leave the device. It does not remove the bank's data-protection obligations.

What this means in practice

- No routine transmission of facial imagery to YEO servers for matching.
- No central YEO biometric database for an attacker to target.
- No requirement for bank operations teams to view raw biometric imagery.
- Bank-defined policies determine when verification operates and how the resulting signal is used.
- The bank remains responsible for its legal basis, customer notices, impact assessment, retention and governance.





Where CFR fits in the banking journey

CFR sits alongside existing KYC, login, payment-risk and fraud-management controls. It adds identity assurance after access has been granted without requiring the bank to replace its existing stack.



Priority use cases

Active digital-banking session

Confirm that the enrolled customer remains present after login

Payment and beneficiary activity

Add identity assurance before or during high-value payments and beneficiary changes

Secure service and communications

Confirm who is accessing sensitive information or issuing instructions

Account recovery

Add identity evidence to a journey frequently targeted through social engineering

Card controls and account settings

Protect actions such as PIN changes, new-device registration and contact-detail changes

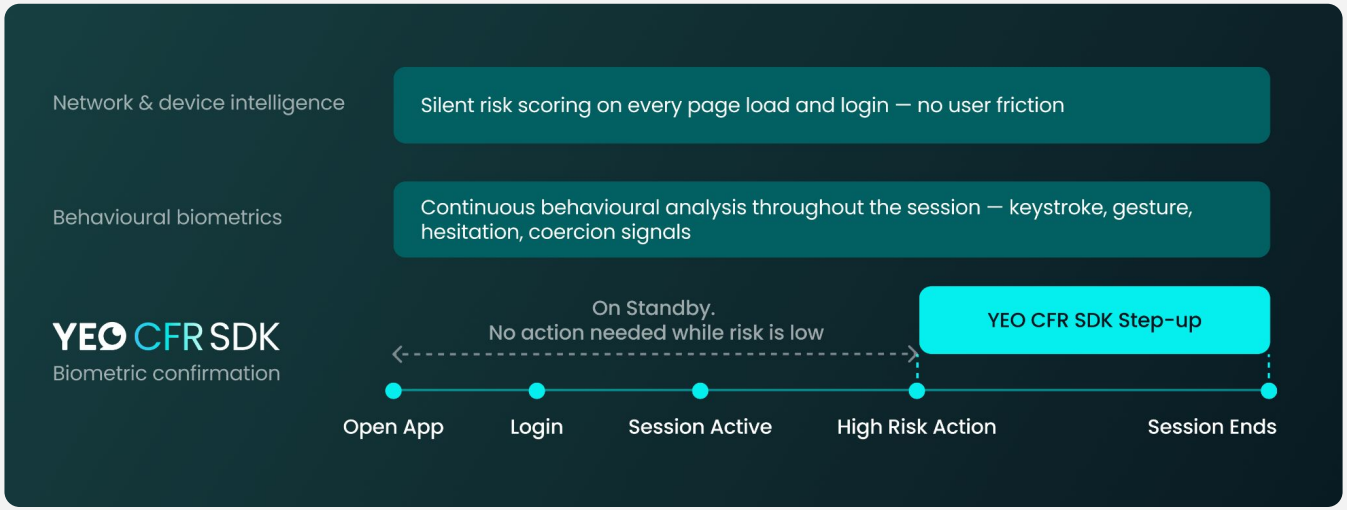
Built to integrate with, not replace the stack.

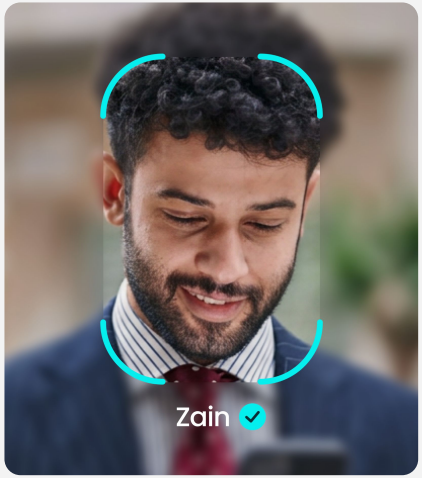
YEO CFR is available for native iOS, native Android, React Native and Flutter environments. It is designed to connect with existing identity, fraud, workflow and case-management systems.

CFR complements existing fraud signals

Banks already use device, network, behavioural and transaction-risk tools. Those tools identify suspicious devices, connections or behaviour. CFR answers a different question: does the person present continue to match the enrolled customer?

A bank can invoke CFR continuously, at selected actions or when an existing risk score crosses a defined threshold. The resulting signal enters the bank's existing decisioning workflow.

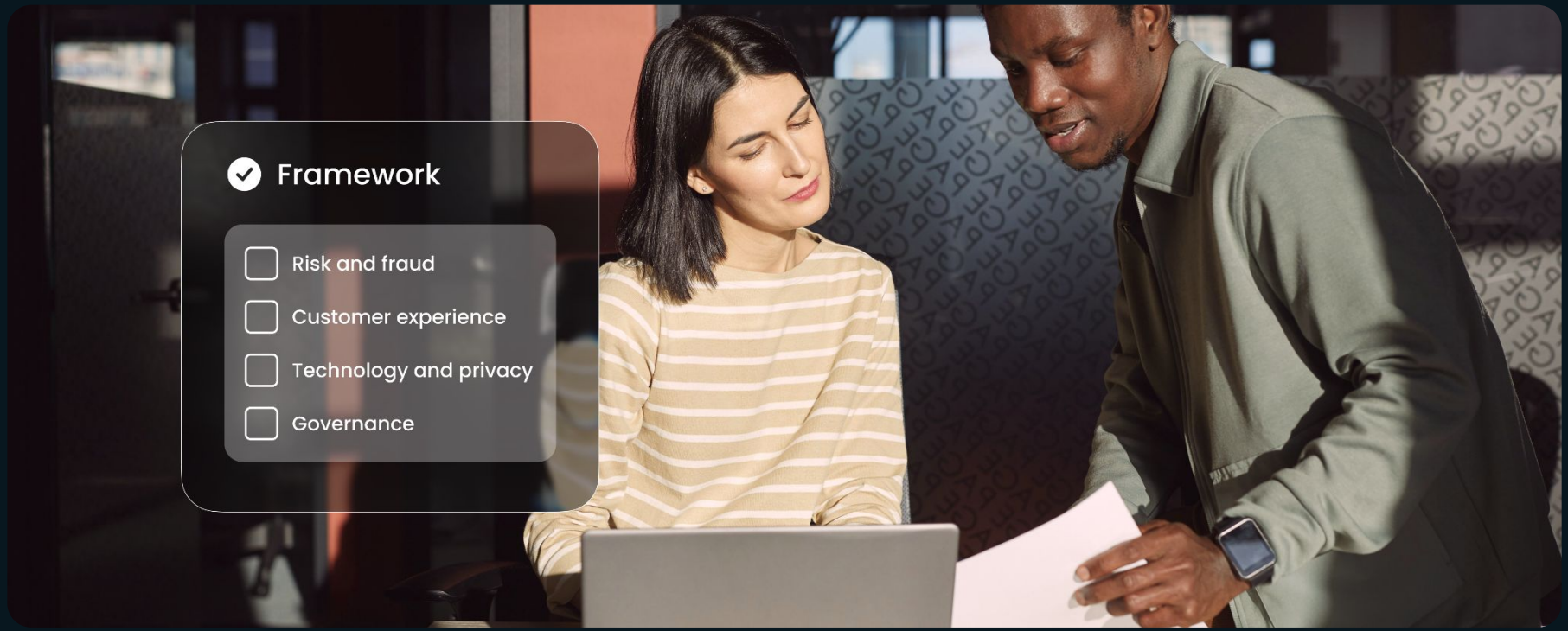




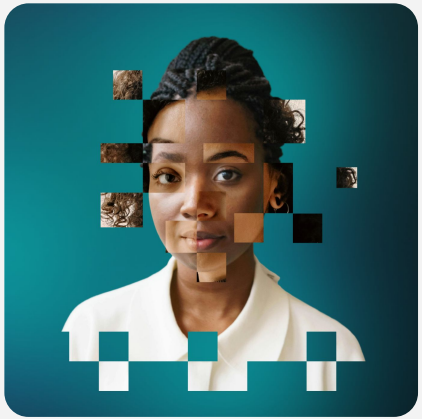


A practical evaluation framework

Banks should evaluate continuous identity assurance against a defined journey, threat model and measurable operating outcome.



Questions to ask



Risk and fraud

- Which losses occur after a legitimate authentication event?
- Which journeys are most exposed to account takeover, session hijacking or unattended-device use?
- What response should absence, mismatch or failed liveness trigger?



Customer experience

- Which challenges are costly, slow or associated with abandonment?
- Where could passive assurance reduce an unnecessary interruption?
- Which customers require an accessible alternative journey?



Technology and privacy

- Where are biometric templates and event records stored?
- How will CFR integrate with identity, fraud and payment decisioning?
- What evidence will be available to risk, audit and incident-response teams?



Governance

- How will the bank document control purpose, testing and residual risk?
- Which complementary controls remain necessary?
- How will the bank measure fraud, friction, accessibility and operating outcomes?
- How should CFR signals enter existing fraud, identity and payment decisioning?

Conclusion

A bank can authenticate a customer successfully and still lose confidence in who controls the session moments later.

KYC establishes identity and authentication controls access. Neither necessarily confirms who remains present throughout a digital journey.

YEO CFR adds a bank-configured identity-assurance signal after login. It can help strengthen session controls, inform fraud decisions and reduce unnecessary challenges where policy, architecture and regulation allow.

It does not replace passwords, device intelligence, behavioural signals or transaction monitoring. It adds the identity evidence those controls cannot provide on their own.

The commercial case can be tested rather than assumed. The next step is to select one high-risk, high-volume banking journey and establish:

- the current fraud-loss baseline;
- the volume and cost of customer challenges;
- challenge-related support demand;
- abandonment and completion rates; and
- the improvement produced by CFR.

The result is a measurable business case for continuous identity assurance — based on the bank's own customers, systems and risk policy.



References

[1] PS23/4 APP scams reimbursement policy statement. https://www.psr.org.uk/app-scams-reimbursement-ps23-4/

[2] Financial Conduct Authority, Consumer Duty. https://www.fca.org.uk/firms/consumer-duty/about

[3] FFIEC, Authentication and Access to Financial Institution Services and Systems (2021). https://www.ffiec.gov/sites/default/files/media/press-releases/2021/authentication-and-access-to-financial-institution-services-and-systems.pdf

[4] Central Bank of the UAE, Consumer Protection Standards. https://rulebook.centralbank.ae/en/rulebook/consumer-protection-standards

[5] Saudi Central Bank (SAMA), Cyber Security Framework. https://rulebook.sama.gov.sa/en/cyber-security-framework-2

[6] FATF | DIGITAL IDENTITY. https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Guidance-on-Digital-Identity-report.pdf

[7] UK Government, Payment Services Regulations 2017. https://www.legislation.gov.uk/uksi/2017/752/contents



YEO CFR SDK

Assess your session-level identity risk

Identify one digital-banking journey where continuous identity assurance could reduce fraud exposure or unnecessary customer friction.

Book a 20-minute banking session-risk review

Book now

yeomessaging.com/industries/banking-finance

