

Case study: myZoi

# API-based cash collateral solution drives financial inclusion in the Middle East

High collateral costs was detracting myZoi from its mission of providing low-cost services to low-income migrant workers in the United Arab Emirates (UAE). Created in collaboration with Standard Chartered, an API-based solution now enables myZoi's customers to use their prepaid cards at a low cost.



[This solution] has really helped us save on potentially a high cost of placing cash collateral for issuing quarantees. As a result of this partnership, Standard Chartered is able to collateralise the transacted amounts in real time in a seamless manner. and myZoi benefits from a scalable solution that enables its customers to continue using their cards seamlessly around the clock.

> Syed Muhammed Ali, CEO, myZoi

## Background

Founded in the pursuit of financial inclusion for all, myZoi empowers underbanked, low-income migrant workers in the UAE with low-cost remittance and payment services. The fintech provides payroll and remittance solutions and wallet services to its customers.

myZoi is regulated by the Central Bank of the United Arab Emirates (CBUAE), with two regulatory licenses issued from the central bank: one for stored value services, and the other for retail payment services. The fintech also intends to expand within the Gulf Cooperation Council (GCC), extending its mission for financial inclusion beyond the UAE.

### Results



Instantaneous protection against settlement risk with the use of automatic escrow



Removal of high-cost requirement of placing a collateral or issuing quarantees to the card network partner.



Customers can easily transact within available balance limits with realtime authorisation. reducing transaction inefficiencies for myZoi.



Ease of solution replication - inherent of the scalable nature of the solution design - as myZoi expands across the GCC region.



This collaboration with myZoi exemplifies how innovative solutions can drive financial inclusion. By embedding our API solution, we've eliminated the need for costly collateral while ensuring secure, real-time payments. This not only enhances transactional efficiency but also supports myZoi's mission of providing affordable financial services to underbanked communities.

Rola Abu Manneh

Chief Executive Officer, UAE, Middle East and Pakistan, Standard Chartered

## Client challenges

To ensure payment settlement following transaction authorisation, card network partners typically require collateral or the issuance of quarantees. While this helps to build commercial trust between financial service providers and their card network partners, it can be very costly. Such requirements were incompatible with myZoi's mission to keep banking costs low for its customers.

#### Solution

Standard Chartered (SC) worked with myZoi to co-create an automated cash-collateral solution to authorise prepaid card transactions in real time. Through its 'payouts-as-a-service' API platform, SC is now embedded into myZoi's transaction flows, collateralising transactions in real time.

How it works: Following a transaction initiation, the API request is approved (dependent on fund availability), and the funds are immediately earmarked and moved from the customer's account to an escrow account. This then enables authorisation of the transaction in real time, and SC manages the onward settlement with Visa.

#### Disclaimer

This material has been prepared by one or more members of SC Group, where "SC Group" refers to Standard Chartered Bank and each of its holding companies, subsidiaries, related corporations, affiliates, representative and branch offices in any jurisdiction, and their respective directors, officers, employees and/or any persons connected with them. Standard Chartered Bank is authorised by the United Kingdom's Prudential Regulation Authority and regulated by the United Kingdom's Financial Conduct Authority and Prudential Regulation Authority.

This material has been produced for reference and information purposes only, is not independent research material, and does not constitute an invitation, recommendation or offer to subscribe for or purchase any of the products or services mentioned or to enter into any transaction.

Some of the information herein may have been obtained from public sources and while SC Group believes such information to be reliable, SC Group has not independently verified the information. Information contained herein is subject to change at any time without notice. Any opinions or views of third parties expressed in this material are those of the third parties identified, and not of SC Group. While all reasonable care has been taken in preparing this material, SC Group makes no representation or warranty as to its accuracy or completeness, and no responsibility or liability is accepted for any errors of fact, omission or for any opinion expressed herein. The members of SC Group may not have the necessary licenses to provide services or offer products in all countries, and/or such provision of services or offer of products may be subject to the regulatory requirements of each jurisdiction.

This material has not been prepared with regard to the specific objectives, situation or particular needs of any particular person, and is not meant to be comprehensive. SC Group does not provide any information technology, accounting, legal, regulatory, tax or investment advice and this material should not be relied on as such. Any comments on information technology, accounting, legal, regulatory, tax or investment matters contained in this material should not be relied on or used as a basis to ascertain the various results or implications arising from the matters contained herein, and you need to exercise your own independent judgment (with the advice of your information technology, accounting, legal, regulatory, tax, investment and other professional advisers as necessary) with respect to the risks and consequences of any matter contained herein. Please note that there have been reports of email phishing targeting bank customers. Please do NOT click on the links in any unusual or suspicious emails, or provide any sensitive personal details, login credentials, PINs, OTPs. We would never ask you to reveal sensitive personal information or passwords, or validate your account over emails, SMSes, or phone calls. If you receive any suspicious emails, SMSes, or phone calls, please call us immediately. Please note that as the recipient, it is your responsibility to check the email for malicious software. SC Group expressly disclaims any liability and responsibility whether arising in tort or contract or otherwise for any damage or losses you may suffer from your use of any fraudulent hyperlinks or use of/reliance on the information contained herein.

You may wish to refer to the incorporation details of Standard Chartered PLC, Standard Chartered Bank and their subsidiaries by visiting the contact us page of our website and viewing our locations.

This material is not for distribution to any person to which, or any jurisdiction in which, its distribution would be prohibited. If you have received this email by mistake, please inform us by email and then delete the message. A translated version in your local language will be made available upon request. Please reach out to your relationship manager to obtain a copy.

© Copyright 2025 Standard Chartered Bank. All rights reserved. All copyrights subsisting and arising out of these materials belong to Standard Chartered Bank and may not be reproduced, distributed, amended, modified, adapted, transmitted in any form, or translated in any way without the prior written consent of Standard Chartered Bank.