mobile connect

How Mobile Connect can transform digital banking

Banks' Authentication Challenge

Consumers like the convenience of being able to bank and transact online using a PC, tablet or smartphone.[1] However, the available authentication procedures involving multiple usernames, passwords, security codes and automated telephone calls can result in a cumbersome user experience.

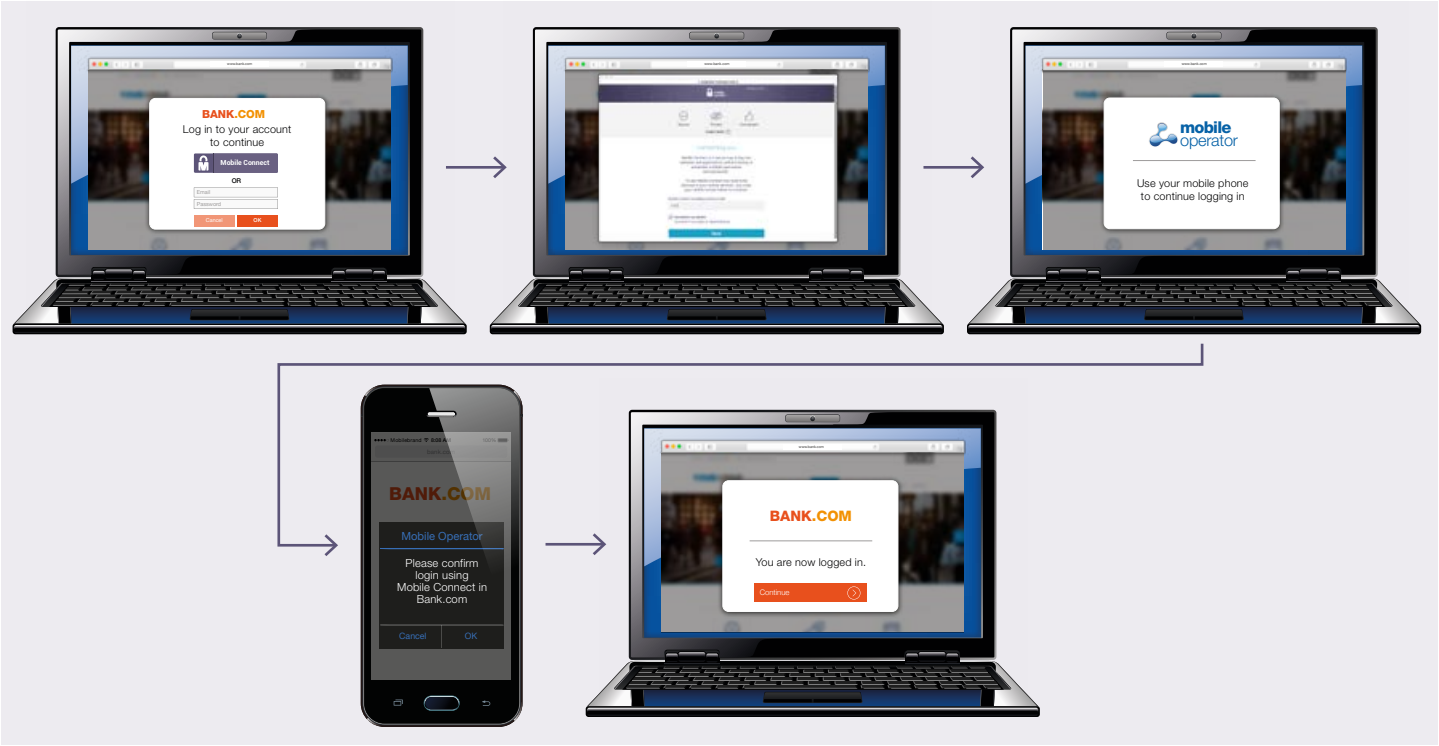
Banks want to be able to interact with customers digitally. Yet, they need to be able to protect their customers from exposure to fraud and identity theft, which is a growing problem as financial services go digital.[2] Although some banks have implemented a proprietary authentication solution, such an approach can be expensive and offer a poor user experience.

Financial services providers are looking for a cost-effective way to reduce friction for online banking and transactions, while increasing security and ensuring compliance with all the relevant regulations.

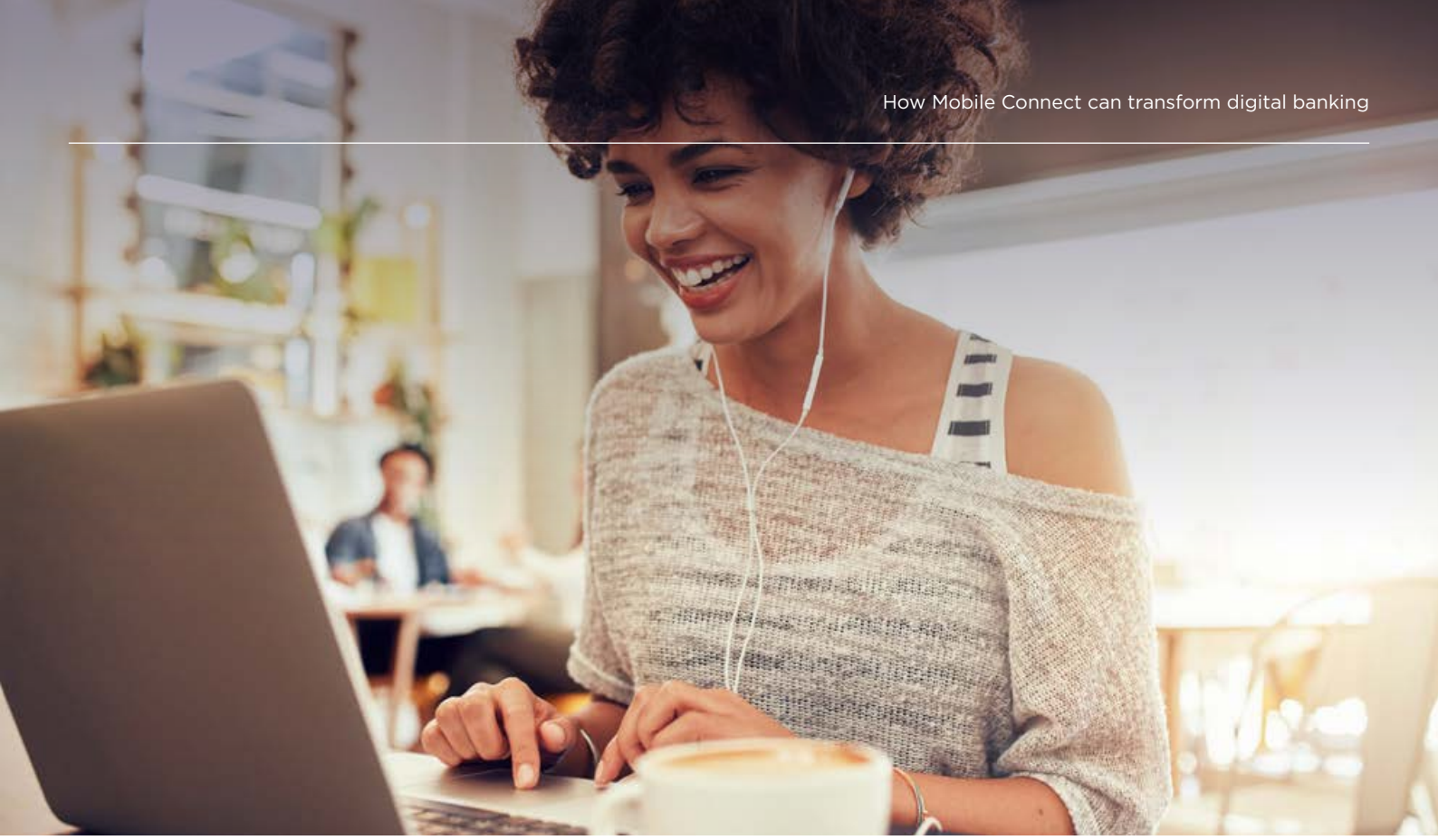
What is Mobile Connect?

Mobile Connect is a mobile-based authentication, authorisation and customer data service that allows simple, secure and convenient access to online services from any device. Combining the user's unique mobile number and device, Mobile Connect enables straightforward and secure digital authentication and attribute sharing.

When a customer selects Mobile Connect to log into their bank's website or app, the service may ask the visitor to input their mobile number in a dedicated window. After this mobile number has been verified, the customer's mobile operator sends a prompt – typically in the form of a SMS or a USSD message – asking them to confirm the interaction as a means of authentication. Once the customer is authenticated, the operator sends the bank a reference token which is persistent and unique to that customer.



1. Nearly two in three Americans use mobile or online as their preferred method of banking: Source Bank of America: http://newsroom.bankofamerica.com/press-releases/consumer-banking/fess-majority-americans-deny-their-smartphone-behaviors
2. Card-related fraud losses incurred by banks and merchants worldwide grew 19% to $16.31 billion in 2014. Source: The Nilson Report: http://www.businesswire.com/news/home/20150804007054/en/Global-Card-Fraud-Losses-Reach-



How Mobile Connect addresses banks' needs

Mobile Connect is a cost-effective authentication mechanism

It makes use of mobile operators' existing assets and is consistent across mobile networks – banks can use the same technical solution and same procedure regardless of the customer's operator or handset. Mobile Connect is also efficient as everything happens online, with the operator acting as the single source of information for that customer.

Mobile Connect reduces friction and encourages interaction

All the consumer needs to authenticate themselves is their mobile phone and SIM, which they already carry with them. This encourages customers to make more transactions and log into their digital banking space more often.

Mobile Connect is secure

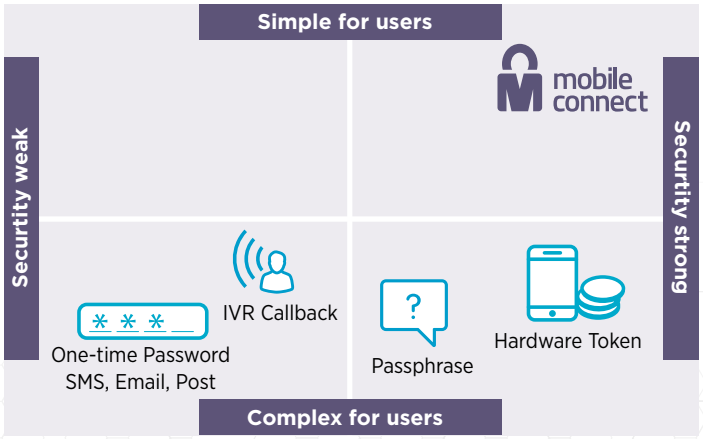
It offers different levels of authentication from simple authentication to multi-factor authentication. The use of the SIM as the first authentication factor makes it extremely difficult for fraudsters to launch an attack at scale. Mobile Connect is also closely aligned with the technical standards being developed by the European Central Bank for strong authentication to meet the requirements of the EU Payment Services Directive regulation. The authentication is implemented through a private secure channel entirely separate from the interaction channel, making it difficult for external parties to intercept credentials.

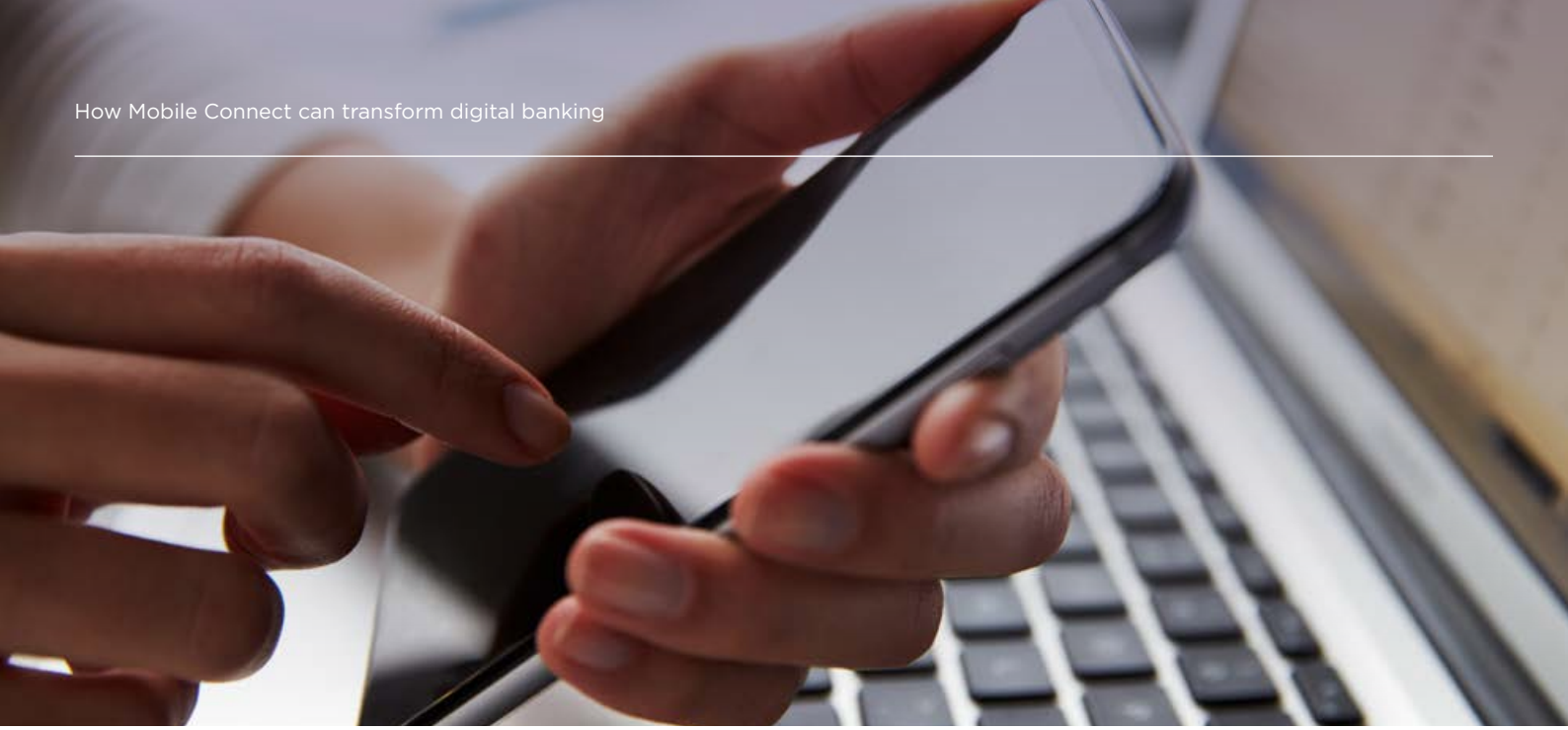
Mobile Connect leverages contextual customer data

Banks can increase security further by leveraging contextual information available to mobile operators. For example, a mobile operator can check whether the handset is in an unusual location or where the user's SIM card is in a new device, helping the bank to evaluate the risk carried by a transaction. Finally, Mobile Connect can be implemented on top of an existing infrastructure, thus enhancing the security, without replacing current authentication or fraud prevention methods.

Mobile Connect enables improved customer insights

Mobile Connect gives the bank a persistent, unique user ID across any channel of customer interaction, generating new insights and enabling innovative new services, which help to position the bank as a progressive market leader.





Example use case: How Mobile Connect can ease online transfers

Banks often require an extra security check before an online money transfer to a new payee is confirmed. In the scenario outlined below, Mobile Connect enables two-factor authorisation to implement this extra security check.

How Mobile Connect can improve the customer experience

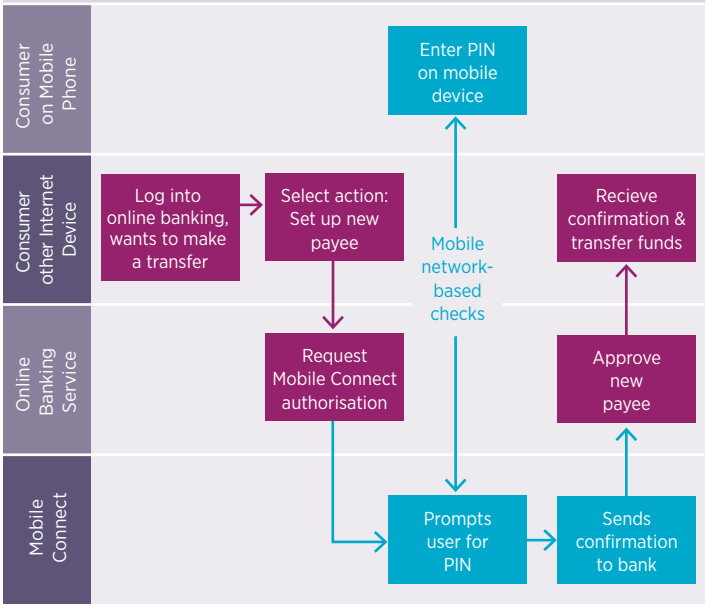
In this scenario, Jim wants to transfer some money to Bob online. Jim logs into his online banking and selects the action to set up a new recipient. As he has already associated his online bank account with Mobile Connect, the bank sends an authorisation request to Mobile Connect. Mobile Connect sends a prompt to Jim asking him to enter his PIN to authorise this transaction. Once the bank receives this confirmation, the bank is confident that it can safely authorise the new payee.

Key benefits over today:

- **The customer only needs to remember their PIN and carry their phone with them.**
- **No need for cumbersome and expensive hard tokens, Interactive Voice Response or One-Time-Password methods.**

Mobile Connect to authorise an online transfer to new Payee

Use case = Strong authorisation



mobile connect

GSMA Personal Data

If you would like more information, please contact GSMA via mobileconnect@gsma.com
GSMA London Office
T +44 (0) 20 7356 0600
www.gsma.com/personaldata
Follow the GSMA on Twitter: @GSMA