

# Common authentication – reducing risk and raising customer service

*As channels proliferate, banks must take a forward-looking approach to combine cost-effective authentication with improved customer service*

*Written by an independent journalist on behalf of ACI Worldwide*



Multiple authentication systems create a number of problems for banks, and these problems will continue to increase as technologies advance. But by thinking creatively about the role of authentication in a multi-channel environment, organisations can begin to leverage these technologies as key to reduce risk and raise customer service.

## **Siloed authentication**

Despite the implementation of more-or-less effective CRM systems, a vast amount of customer information remains siloed. This is due to incompatible data formats and inefficient communication across different channels and areas of financial services. This situation is complicated again by the presence of multiple authentication procedures that have been developed for various banking channels at different times. The authentication systems for branch, ATMs and mail-order/telephone order (MOTO) transactions were often centralised 20 or even 30 years ago. But the advent of online and mobile transactions has led many banks to develop their own e- and m-authentication systems, creating multiple, incompatible procedures.

## **Off-putting for customers**

Incompatible authentication systems hamper existing customer service by increasing the risk of inconsistent service across channels, as well as creating barriers to new technologies and bank strategies. Multiple registrations are off-putting and difficult to manage, as Herman Singh, director of online business at Standard Bank of South Africa, says: “If you require customers to authenticate themselves differently on each of the services they need, forcing them to remember five different passwords, you’re likely to create a significant resistance to using those services, and hence an obstacle to rapid adoption.”

## **Dangers of poor customer information**

The situation is made worse by the loss of crucial customer information: customers may register for multiple services without the

institution achieving a single customer profile. This risks compromising service, and also exposes banks to increased fraud.

Crimes such as identity theft exploit patches of poor communication between banking channels and data repositories. As the world becomes increasingly networked, individuals’ digital identity is distributed throughout many different locations. Identity theft exploits this wide distribution and incompatibility of different repositories of customer information to steal individuals’ personal details. This information is then used to obtain goods and services or commit crimes such as money laundering. Genuine customers may not realise their identity has been stolen for months or even years.

**Andy Brown, senior product manager at ACI, says:**  
“If people don’t have a consistent mechanism across all channels, fraudsters are going to get in there. For example, I have heard of wallets being stolen, and the debit card being used to withdraw money over the counter in a bank. Since teller staff don’t ask for a PIN or identifier other than an unreadable signature, the assumption seems to be ‘if they’ve got the card, they’re OK.’”

## **Moving forward**

So how are banks to maintain a consistent view across multiple channels, customers, products and services? One strategy is to centralise the acquiring, authentication and authorisation stages across all banking channels. Information would thus be better integrated and more consistent, helping banks to combat identity fraud through easier cross-referencing of customer data and transaction history.

Identity theft can also be tackled by changing processes. For example, when banks receive a letter requesting a change of address, it is common to update the customer’s details without further security checks. But

# Common authentication

changed processes, such as a telephone call to request a second method of authentication, would help to reduce the risk of identity theft.

EMV compliance (obligatory in EMEA from 2005) will also strengthen the set of available authentication methods. EMV-compliant chip cards provide a secure token that then becomes part of the identification method. This can be used across a number of channels, not just at ATMs and the point of sale (POS). For example, EMV security could be used at a bank branch. In this scenario, the intelligent chip on the card would become the main source of identification, reinforced by the provision of a PIN pad for the customer to enter their number. But the true benefits of this extra layer of authentication will be realised when it is properly integrated with the other possibilities, and configured to work across channels. A possible application of EMV could then enable online shoppers to buy at home using an EMV card reader and PIN pad attached to a home PC.

As forms of authentication become ever more numerous, and fraudsters become ever more ingenious, banks must combine cost-effective security with customer service. Singh argues that for banks to achieve this, rationalisation is inevitable: "As channels, features and functions proliferate, the aggregated plethora of identifiers and authentication methods will become increasingly unmanageable. It is also clear that migration to direct channels is a strategic imperative for many financial institutions, and we have to make that migration as convenient as possible for our customers. Basically, what we need is technology that helps converge multiple identifiers onto a single level."

**Denys Whitley, project manager, group IT at Ulster Bank, agrees. "Consolidating authentication systems is something that will be inevitable for banks," he says.**

## New thinking

So, if identification technologies are to be converged, what is the best approach? Adapting an existing system, or plugging in a new one? Will banks have to tear out all their existing technology and start again? The good news is that nothing this radical is required. But addressing the growing need for platform- and channel-independent access technologies will require a rethink of existing systems.

The first step is familiar. Many organisations have multiple registration points and registration engines, and information is not shared between

systems, exacerbating the poor re-use of information. This must be rectified through consolidated customer data including a single view of all the services for which a customer is registered.

Once customer data and registration information have been properly co-ordinated, applications need to be reconfigured until identity can be shared between applications. Singh explains: "Most institutions have systems where the authentication is integrated into the application itself. There's a different protocol, different identifiers and authenticators for each service. If a customer phones up an Interactive Voice Response service (IVR), there'll be a specific authentication for the IVR. If the customer goes online, there's an authentication layer there. If a customer goes to an ATM, there's one there. In every case, it's a separate authentication layer using different identifiers."

However, object-oriented programming can help address this problem, creating applications that separate the authentication layer into a separate object, in a loosely-coupled system. These identify common objects within application code, and share them between different applications.

**"If you were building an IVR system for banking, and an e-banking system, each would have a user interface, registration, identification, transfer, payments, beneficiary loading functionalities. To avoid having to build the same functionality twice, you could build it once and share it – each application uses the same object, and hence the same data to authenticate the customer," Herman Singh, director of online business at Standard Bank of South Africa.**

## Are there any risks?

The potential benefits are obvious: simpler systems, streamlined processes and centralised data are all goals that banks continue to pursue. But are there any risks? If there is a single point of entry, this must also represent a single point of failure? If fraudsters only need to crack one identifier, will this not make the banks more vulnerable?

Authentication systems are always part of a wider set of controls and security measures. Singh describes the security measures in place at the Standard Bank of South Africa: "We use a number of compensating controls such as pattern recognition and fraud detection software, as

# Common authentication

well as rigorous control of payment limits — and this is merely to describe one or two levels of a 12-level security system.”

An emerging strategy is the use of multiple identification levels. For example, when a customer logs in to a bank’s Internet channel, they can be asked for a password, an account number and a PIN number. This might then be followed by an SMS message to the customer’s mobile phone, informing them that their e-banking account has been activated. In fact, rather than increasing vulnerability, the single repository of customer information can play a powerful role in combating fraud, as Brown points out.

**“The more consistent and centralised the customer’s data is, the easier it is to ensure that they know what is happening to their account, through email or mobile alerts. This helps close some of the loopholes that the fraudsters can currently exploit,” Andy Brown, senior product manager at ACI Worldwide.**

## **Truly integrated authentication**

Common authentication on its own is not a solution to fraud. But authentication systems of the future will become increasingly unmanageable unless rationalisation takes place – and if this does not happen, customers will simply ignore new services or take their custom elsewhere. Instead, a set of identifiers can be used to create truly integrated authentication systems that leverage common customer data not to increase vulnerability, but to combat it through cross-channel customer transaction alerts and other anti-fraud measures.

Authentication must be balanced by robust anti-fraud measures, and any authentication system is only a part of a wider fraud scoring and risk management strategy. But if it is properly done, it will lower the costs associated with fraud, and also help banks to improve customer interaction through consistent service and more efficient transaction processing. This, in turn, will strengthen both a bank’s brand and customer satisfaction.