CASE STUDY

GSMA Device Check™

How SLC Digital deploys GSMA Device Check to help banks tackle identity fraud

Published by

MOBILE WORLD LIVE

In partnership with

GSMA Industry Services

For many years, resellers and insurance companies have used GSMA Device Check to identify stolen and fraudulently obtained devices. Now tech firm SLC Digital has developed a new application of the tool: helping banks fight customer impersonation scams.

Every year, criminals steal up to 90 million smartphones. These thefts are heartbreaking for the victims and costly for the industry. So, what can be done? One obvious solution is to make it harder for criminals to recycle stolen devices. How? By giving any company that handles second hand devices – mobile network operators (MNOs), resellers, insurers and retailers – the ability to identify stolen or lost goods.

What is GSMA Device Check?

Most mobile devices (phones, tablets, etc) have a unique identifier known as the IMEI (International Mobile Equipment Identifier). The GSMA's Device Registry database lists IMEIs and also maintains a 'Block List'. The latter comprises all IMEIs that MNOs, manufacturers, re-sellers and marketplaces have reported as lost, stolen or tied to an unpaid balance.

So, how can organisations access the Block List database?

Users simply subscribe to Device Check, and then inspect the database via a web-based dashboard or API. When they enter an IMEI, they can see if the device has been flagged for any reason.

Device Check is now well-established. Companies all over the world have used it to successfully fight device theft for nearly a decade. Law enforcement and regulators can also access the database for free.

But new use cases are constantly emerging. The latest centres on financial services, with US tech company SLC Digital using Device Check to help banks fight skyrocketing rates of fraud and account takeover (ATO).

Let's find out more.

Online banking's big challenge: account take over scams

Digital finance has made life easier for millions. With a 'bank in your pocket', account holders can cut out time-consuming branch visits, long queues and paper forms.

But there's a downside: fraud. In the absence of face-to-face transactions, it's harder for banks to authenticate customers reliably. This has given criminals the opportunity to use technological hacks and social engineering scams to perform account takeovers. Indeed, US adults alone lost $47 billion to identity fraud in 2024.

So, what exactly is account takeover fraud?

ATO happens when criminals gain access to a customer's account without permission. Typically, they go through two steps. First, they gain access to the victim's account using stolen information or through SIM swap, port-out fraud or other account recovery exploits. Once they have access, they make changes to the account such as:

- Changing the victim's personally identifiable information
- Requesting a new card
- Adding an authorised user
- Changing the password

The fraudsters then make unauthorised transactions that appear legitimate. Alternatively, they might sell on the customer's data.

A robust defence against ATO: SIM-based authentication

Thankfully, there is a strong defence against ATO attacks: SIM-based authentication. This method gives banks the ability to inspect a user's SIM card activity. They can then look for indications of fraud such as a recent SIM swap, device changes, location patterns and behavioural anomalies.

The SIM's cryptographic 'signature' is highly secure. Its unique combination of mobile phone number and associated SIM card identity (IMSI) is not vulnerable to phishing.

The end-user experience is superior too. With SIM-based ID, customers are passively verified. There are no passwords or SMS codes to type in. Identity is anchored to the SIM/eSIM secure element rather than shareable credentials.

SLC Digital's eSIM and API solution

SLC Digital is a specialist in SIM-based identity verification, supporting a secure confirmation layer that operates outside traditional apps, phone numbers and messaging channels. The company provides enterprise customers with eSIMs and network APIs, which they can use to monitor their customers' live network status. If they detect any suspicious activity, they can suspend, revoke or even issue a new identity without requiring any manual action from the user.

So how does this work in the financial services context? Well, when an account holder signs in or makes a transfer etc, the bank can study a wide range of real-time signals. It can check for anomalies such as SIM swaps, number ports, roaming, GPS spoofing and more.

Beyond identity verification, SLC also allows enterprises to confirm high-risk actions through a protected, out-of-band channel. Because the confirmation and signalling occur at the network and SIM layer, the channel remains invisible to attackers and unaffected by malware, phishing or compromised devices. This significantly reduces the risk of account takeover and transaction fraud.

SLC currently has access to more than 600 mobile networks in more than 180 countries. This means enterprises can upload and manage eSIMs virtually anywhere. Customers can track their eSIMs on real-time dashboards with customisable views.

Edwin Candy, formerly Technology Director at Orange and now an adviser at SLC Digital, believes SIM-based ID can transform the digital identity space. "The SIM card already solved the problem of ID in the telco industry," he says. "And now it could solve the identity problem for the world, because there are 6 billion mobile phones out there. SIM-based ID moves the way we authenticate people from a probabilistic model to a deterministic one. Essentially, you are the phone."

Travis McGregor, CEO of SLC Digital, agrees and expects SIM-based ID to shake up digital banking. "Combining live network data and information from our own eSIMs lets us authenticate devices and users from the silicon up. This is a new trusted foundation for secure communication. When chip and PIN came in for face-to-face payments, counterfeit card fraud went from very high to zero. I believe SIM-based identity verification will do the same for digital transactions."

How SLC added Device Check to boost bank defences

SLC's combination of eSIM and network APIs provides banks with a robust tool for flagging active suspicious activity once an eSIM is in use. But what about the on-boarding part? How can SLC ensure that the device itself is legitimate?

Early in 2025, SLC found the answer: it integrated Device Check into its solution to verify the hardware housing the eSIM.

Numan Maloney, head of Product at SLC Digital, describes how the process works. "When we get the green light to put an eSIM onto a new device, we need to check the status of the device first," he says. "So as soon as the eSIM is live, we ping it to find out the IMEI. Then we take that IMEI and plug it into GSMA Device Check. Within a second, we have really useful, actionable data to determine whether or not someone is on a risky device."

"And we can repeat the process every time there's a high risk transaction such as a transfer or a loan application. We then forward the information onto the client and they can combine it with other data to make a decision about whether the customer is trustworthy."

To further bolster on-boarding security, SLC's process also includes biometric checks. In October 2025, it formed a partnership with biometrics specialist IDEMIA to authenticate customers at sign-up.

Amit Sharma, Head of Digital Strategy at IDEMIA Public Security, believes the combination of its biometric tools with GSMA Device Check can deliver unmatched security. "Linking verified human and organisational identities with secure device signals strengthens fraud prevention at on-boarding and authentication by adding more deterministic signals and real-time protections. It means enterprises can make higher-confidence decisions in real time without adding friction for users, while maintaining strong controls over sensitive personal data."

SLC is now working on pilots with banks, blockchain networks and global enterprises. These projects are part of a broader ecosystem that unifies all stakeholders into a single deterministic identity and trust layer. They include sandboxes with a range of financial institutions participating in the Canton blockchain network.

Pinar Emirdag, Industry Partner at 7RIDGE, an investor in Canton Network, has high hopes for the combination of SIM-based authentication and tokenised real-world assets."On-chain finance is maturing fast and enabling new business models. I believe that SLC's eSIM-anchored device identity tech can provide these new services with a native, end-to-end foundation for secure transactions."

Beyond financial services, SLC is also in discussions with healthcare and other high-risk sectors to explore how its SIM/eSIM-based identity and API services can strengthen security across their digital ecosystems too.

Tyler Smith, head of Managed Services at the GSMA, welcomes SLC's creative application of Device Check and is confident it can accelerate a SIM-based approach to security in financial services. "We're delighted to welcome SLC. It is showcasing an excellent example of how telecoms can come together with fintech and banking to provide additional security for consumers."

Your next step

This partner study reveals an exciting new use case for GSMA Device Check. It shows how, in combination with SLC's SIM-anchored identity, the service can deliver a new class of deterministic trust for high-risk digital transactions.

Can GSMA Device Check solve your business challenges too?

If you would like to know more, please complete this form.

A quick guide to GSMA Device Check

What is Device Check? And why is the GSMA uniquely positioned to curate the world's most comprehensive database of mobile devices?

The GSMA is the mobile industry's representative body. Its members comprise more than 750 mobile network operators and nearly 400 ecosystem companies (device makers, software specialists, equipment providers, etc).

One of the GSMA's core services is its comprehensive Device Registry. It employs the unique 15-digit IMEI to identify and track the status of a device.The first eight digits of the IMEI are from the TAC (Type Allocation Code), which relates to the device model.

Two groups contribute information to the database. They are Contributor Network Operators (CNOs) and Contributor Third Parties (CTPs) – comprising approved organisations that own device inventory, such as manufacturers, resellers, insurers, marketplaces and others.

The registry comprises the following data fields:

- Device information such as make, model type and other, associated with the IMEI
- Block List status
- Block List history
- Submission date, country and contributor responsible for the entry and reason code (if blocklisted)

The GSMA, in collaboration with key industry players, created Device Check to let third parties query the current and historical status of a device. Every check will return either a 'Green' status with the message 'NO - not flagged on GSMA Block List'. Or, if the device has been reported lost or stolen, a 'Red' status with the reason displayed in the Device History.

But the adoption of Device Check is constantly growing. Today, the tool helps hundreds of companies globally to query the status of devices. More than 170 million devices have been blocklisted.

And in 2025, there were more than 150 million look ups.

Historically, most users of Device Check have been either resellers, insurance companies or law enforcement. Resellers and insurers deploy the service to:

- Look up whether a device has been reported as stolen or fraudulent
- Provide fast confirmation of exact model and status (with ten attributes)
- See whether a device has an existing financial or ownership claim
- Help calculate replacement value

Meanwhile police access Device Check to investigate lost/stolen devices, including repatriation of devices and identifying criminals linked to robberies.

GSMA Industry Services

GSMA Industry Services

As part of the GSMA, the global organisation that unifies the mobile ecosystem, we work closely with the mobile ecosystem to identify network and device challenges that are currently having a negative impact on their business, customers and industry reputation.

GSMA Industry Services are here to deliver services that improve the performance, interoperability and security of networks and devices.

Crucially, as part of this, they run the GSMA Device Registry, a global database of IMEI numbers. By using GSMA Services, that IMEI number can tell you whether a phone has been reported lost or stolen, what networks it is compatible with around the world and whether the device is subject to ownership or financial claims.

Find out more at gsma.com/services

MOBILE WORLD LIVE

Mobile World Live is the premier destination for news, insight and intelligence for the global mobile industry. Armed with a dedicated team of experienced reporters from around the world, we are the industry's most trusted media outlet for breaking news, special features, investigative reporting, and expert analysis of today's biggest stories.

We are firmly committed to delivering accurate, quality journalism to our readers through news articles, video broadcasts, live and digital events, and more. Our engaged audience of mobile, tech and telecom professionals, including C-suite executives, business decision makers and influencers depend on the unrivalled content and analysis Mobile World Live provides to make informed business decisions every day.

Since 2016, Mobile World Live has also had a team of in-house media and marketing experts who work directly with our brand partners to produce bespoke content and deliver it to our audience in strategic yet innovative ways. Our portfolio of custom work - including whitepapers, webinars, live studio interviews, case studies, industry surveys and more – leverage the same level of industry knowledge and perspective that propels our newsroom.

Mobile World Live is published by, but editorially independent from, the GSMA, producing Show Daily publications for all GSMA events and Mobile World Live TV – the award-winning broadcast service of Mobile World Congress and home to GSMA event keynote presentations.

Find out more at www.mobileworldlive.com