SIM swap fraud is getting worse – but now there is a solution

If you are a fraud or risk manager, or responsible for user identity management, you probably know that SIM swap fraud is a big problem – and it's growing. But you may not realise that there is now an easy and secure solution, which can both protect your users and streamline authentication.

In this article, we look at how common mobile user authentication approaches are allowing SIM swap fraud to proliferate, explore the specific mobile vulnerabilities that enable SIM swap fraud, and lastly, explain how a new, mobile-native approach can finally solve this problem.

Who is at risk from SIM swap fraud?

SIM Swap fraud is a widespread issue. In broad terms, any business that uses SMS 2FA is at risk. It may be your highest profile or most valuable customers who are targeted first, but in reality, all of your users are at risk.

While banks, fintechs, and crypto businesses have been particularly targeted, the risk is also very significant for any mobile app that relies on the mobile number as the primary user identity. The good news is that, if you are in any of these categories, there is now an easy solution.

Why is this a problem?

We've all become accustomed to using email + password (a 'knowledge' factor) when registering for a new online account.

However, knowledge factors such as passwords are now widely understood to be a flawed security solution, because knowledge can be shared – and leaked. Consequently, SMS OTP (one-time password) is often added as a second ('possession') factor. Unfortunately, that is just a 'sticking plaster' on top, with its own vulnerabilities which create new attack vectors for bad actors.

Because of the way SMS 2FA is used as a security layer when changing a password, compromising that SMS channel gives bad actors wide-ranging access to multiple

user accounts, with serious potential consequences in terms of financial theft and stolen identities.

How does the fraud work?

Here is what typically happens:

1. A bad actor finds out the victim's mobile number and some personal information, typically via a phishing scam, social engineering, or buying information from other criminals.
2. They use that information to impersonate the victim to their mobile network operator (MNO), saying that they need a new SIM card – perhaps pretending that they lost their phone.
3. The MNO customer support agent issues the new SIM card to the bad actor, with the victim's mobile number mapped to it.
4. As soon as that SIM card goes live (is activated in the bad actor's mobile phone), the victim's original SIM stops working.
5. Before the victim notices, or before they do anything about it, the bad actor quickly logs into their online banking, social media, email, and more, and changes the password by intercepting the PIN codes sent out by SMS. They can then easily steal the victim's identity and all of their money.

SIM swap fraud is, unfortunately, a simple and successful method with a thriving community of criminals behind it, and it is spreading rapidly. The good news? There is now a simple fix.

A new and easy solution: SIM-based authentication

SIM swap fraud relies on the bad actor possessing a newly-issued SIM card that has the target user's mobile number mapped to it. However, each SIM card has a unique identity number (called the International Mobile Subscriber Identity, or **IMSI**).

This means that if a new SIM card is issued to a bad actor, the IMSI of that new SIM card will be different to the IMSI of the original SIM card owned by the target user. That difference makes it possible to detect and avoid SIM swap fraud.

The technology which authenticates the identity of each SIM card is a core part of every mobile network – it's how MNOs are able to bill us correctly for our mobile network usage. But it is only now becoming available for identity management and fraud prevention. We call this new approach SIM-based authentication.

How does SIM-based authentication actually work?

tru.ID offers a range of productised APIs for SIM-based authentication, which work across MNOs and support different identity management and fraud use cases.

Assuming your user has registered and you already have a validated mobile phone number, you can use tru.ID Active SIMCheck to verify that the SIM card has not changed before you send the user an SMS OTP. Your app or site passes the verified mobile number to tru.ID via our API, and our API provides you with an immediate response. If the registered user is still in possession of the same SIM card, the check will come back positive, and you can send the SMS OTP as normal. But if there has been a change of SIM card, the check will fail, and you can follow your step-up security flow.

What's more, if you are looking for a SIM swap fraud solution for new users which also greatly improves UX, tru.ID offers Strong SubscriberCheck, which combines frictionless SIM-based authentication of the mobile phone number (without needing an SMS) with the silent check that the SIM card has not changed. This means your onboarding flow can be as simple as possible, resulting in delighted users without losing security.

The benefits of SIM-based authentication

SIM-based authentication fixes the core SMS OTP vulnerability which enables SIM swap fraud. But it also has significant additional benefits, which can dramatically increase mobile registration rates and solve user identity management challenges.

Unrivalled security: A SIM card comes with impregnable cryptography and is the same piece of highly secure, scalable and proven microcomputer technology that you can see in every credit card. Mobile phone numbers are also uniquely tied to an

individual SIM card. At any one time, this pairing of mobile number + SIM card is entirely unique, not duplicable, and cryptographically secure.

Seamless mobile number verification: For a user, the experience is extra simple – they just type their mobile number as usual, and both mobile number and SIM card identity are verified instantly, with no further action required: no SMS to wait for, no PIN code to retype.

Potential to replace passwords: In addition to securing SMS 2FA, SIM-based authentication opens the door to a far bigger opportunity – the chance to finally move away from passwords. You can transition to a far more secure solution, using a mobile-native 'possession factor' (the SIM card) together with on-device biometrics. tru.ID can support you in this transition. To find out more, contact us to speak to one of our experts.

How to get started

Solving SIM Swap is fast and easy with tru.ID. Our products are easily integrated into any client-server application architecture using restful APIs along with iOS, Android, React Native, and Mobile Web SDKs.

If you plan to keep using SMS 2FA, **Active SIMCheck** is the best way to secure your user base against SIM swap fraud. If you prefer to move away from SMS 2FA and want a more secure, mobile native authentication, then choose **Strong SubscriberCheck**.

Developers can find all they need to get started on our website, including integration guides for all our products, which can be found in our documentation. To get started, simply sign up and start testing for free today.

Set up a demo, speak to an expert, or learn more

If you would see our products in action, schedule a demo, or speak to an expert, simply contact us

For all the latest from tru.ID, follow us on LinkedIn and Twitter.