New SIM swap check from tru.ID, the mobile authentication platform, stops the growing menace of SIM swap fraud

Tuesday 8 June, 2021

Active SIMCheck from tru.ID cuts the risk of SIM swap fraud with real-time SIM change detection before an SMS is sent. Built to work alongside any existing 2FA solution.

Authentication platform **tru.ID** (https://tru.id) has released **Active SIMCheck**, an easy to integrate API product, as a timely response to the alarming growth in SIM swap fraud and account takeovers. Banks, FinTechs, and any company using SMS to send security PIN codes, are all at risk.

Many kinds of mobile fraud, including SIM swap, are now becoming mainstream. Just recently, Wired UK reported on the “relentless rise” of Royal Mail text message scams, while The Sun warned against WhatsApp scam access codes. According to Javelin, the strategy and research firm, there’s been a 72% year-on-year increase of account takeover fraud (2020).

By using **Active SIMCheck**, any online business that uses PIN codes sent by SMS for user authentication can now protect their customers and their brand from the potential damage of identity theft and account takeover caused by SIM swap fraud.

One of the most common ways to implement SIM swap fraud is to intercept an SMS PIN code, and then take over a customer's account.

Now there is a simple, turnkey solution - Active SIMCheck from tru.ID - which works for any business that uses SMS PIN codes for user authentication.

How tru.ID Active SIMCheck works
tru.ID Active SIMCheck is an API-based service that connects directly, and in real-time, to mobile network operators to verify the identity of the SIM card in a user’s mobile phone. If there has been a recent change to that SIM card, the API will flag the change before an SMS or password reset code is sent, enabling action to be taken and blocking potential fraudsters from intercepting SMS messages including SMS 2FA PIN codes.

The new security check can be integrated quickly and easily alongside existing SMS 2FA solutions. There is no need for any change to user experience.

Paul McGuire, co-founder and CEO of tru.ID, says:
"Many of the security challenges faced by businesses today are caused by outdated reliance on passwords and SMS PIN codes. tru.ID delivers user authentication that is mobile-native, seamless, secure and private. Active SIMCheck is part of the range of new mobile authentication products developed by tru.ID that are based on the cryptographic security of the SIM card. The difference with Active SIMCheck is that it enables businesses to solve for a major fraud risk without impacting the user experience."

About tru.ID
tru.ID (https://tru.id) is an API platform for mobile Authentication-as-a-Service.

Using the cryptographic security of the SIM card, tru.ID unlocks a whole new way of doing business online using just a mobile phone number. App developers can use our APIs to innovate the mobile user experience, helping to increase revenues and reduce fake accounts and fraud.

tru.ID is available in 15 markets (including UK, Germany, Spain, France, Netherlands, Canada, USA, India and Indonesia) and covers over 3 billion mobile users.

tru.ID was co-founded by Paul McGuire and Eric Nadalin, both serial entrepreneurs with deep mobile expertise. Paul previously co-founded mBlox (acquired by Sinch) followed by Boku (AIM:BOKU) and Eric was co-founder of iPin (acquired by Valista) and Nexmo (acquired by Vonage).

Find out more at tru.ID, on Twitter or LinkedIn.

-- APPENDIX --

Media:

Related Sectors:

Computing & Telecoms :: Crypto Currency ::

Related Keywords:

Sim Swap :: Sim Swap Fraud :: Cybersecurity :: Sms 2fa :: 2fa :: Two-Factor Authentication :: Mobile Identity ::

Scan Me:

Who is at risk from SIM swap fraud?
Consumers' general reliance on m-commerce, and other online interactions for banking, health and education has been accelerated by lockdowns - and fraudsters have taken advantage. Now it is not only high profile cases, such as Twitter CEO's Jack Dorsey account takeover, or tech entrepreneur Robert Ross' $1million life-saving losses on crypto, who are targets of fraudulent activity. The customers of every business that uses PIN codes sent by SMS are now at risk of having their identity taken away and their savings stolen.

Why has SIM swap become such a big issue?
Most phone-based authentication methods today simply use the mobile number, and rely on a PIN code that is sent via SMS, or a voice call. Companies assume this is a possession-factor authentication method, but the problem is that it doesn't reliably prove possession. There are some fundamental flaws – and bad actors are taking advantage.The primary issue is SIM swap. Bad actors are increasingly committing SIM swap fraud by persuading the mobile operator to issue them with a replacement SIM card that takes over the same mobile number. They are then able to receive all voice calls and SMS messages (including PIN codes) sent to that number, and then use those codes to take over that User's accounts. There are many other issues with SMS 2FA; for a full comparison take a look at the SMS 2FA security analysis on our website.

The solution? SIM-based authentication
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, and tru.ID makes it available via API for fast and easy integration.

Company Contact:

_

tru.ID

E. natalie.malevsky@tru.id
W. https://tru.id

View Online

Additional Assets:
https://tru.id/products/active-simcheck

Newsroom: Visit our Newsroom for all the latest stories:
https://www.tru-id.pressat.co.uk