Sim Swap for PSD2 from Lusis Payments

Author: Chris Curd

It is widely accepted that the need for banks to have a solution compliant with PSD2 by 31st December 2020 is proving a real challenge. In fact, banks and financial institutions must have a solution in place and working as soon as possible to show the payment directive that they will be compliant by go live. In September 2019, an update to the PSD2 required banks to ensure that a SIM card had not been compromised while conducting mobile banking and/or payment transactions.

While this is an excellent step forward for the future of mobile banking security, it does mean that banks throughout the EU will need to implement new SMS safety measures that use the latest technology, which can. be expensive. The mobile phone is now the most used device for all types of activity, with over 65% of all transactions, on or off WIFI. Fraudsters taking advantage of this as a major opportunity to 'hack' into accounts and expose the banks and consumers to fraud. For the first time the bank data will be exposed more at the end consumer.

There is a great deal of discussion in the marketplace around this requirement, which asks for additional checks to be implemented ensuring the security and ownership between the SIM and the Phone itself. The question on many banks' minds is “How to deploy a Sim Swap check quickly and effectively to make me compliant with PSD2?”.

Read on to see how Lusis has created a low cost, rapidly, secure solution.

What is Sim Swap Fraud?

SIM swap fraud relates to a mobile phone user changing the phone's Sim Card (e.g. change of Service Provider) whilst retaining the same mobile phone number – known as Porting.

Phone Hackers use a technique to take control of the user's mobile phone number to obtain sensitive information from individuals' private data (e.g. bank accounts). The PSD2 directive serves to eliminate this hacking and fraud

through specific checks to ensure the mobile phone, SIM and owner are all secure. This is the service that Lusis offers.

In recent years SIM swap fraud has become increasingly prevalent. According to an investigation by" Motherboard", a SIM swapping operation is "relatively easy to pull off" and has indiscriminately affected people irrespective of their geographic location around the world. Another motivation for fraudsters is how difficult it is to prevent. If the hacker is able to provide all of the information necessary to "prove" that they are the victim, it can be difficult for carriers to distinguish between a hacker posing as a user and a genuine user. It can also be difficult to track perpetrators of SIM swapping, so there is little risk and high reward for those willing to take advantage of individuals.

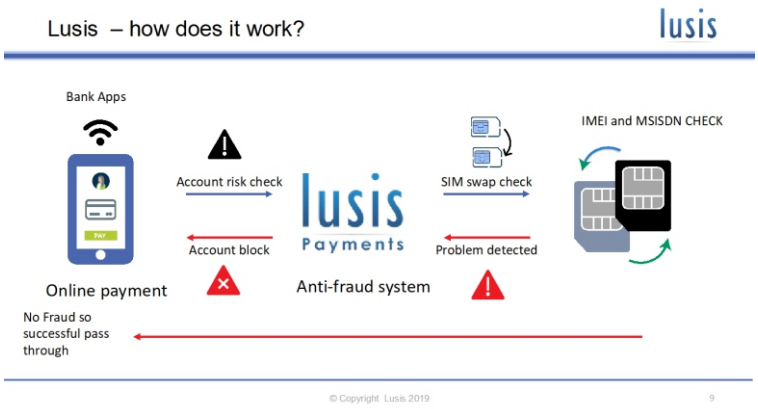
So how to STOP this from effecting YOU?

Lusis SIM Swap Protection Service

Customers of financial institutions are generally at the highest risk for SIM swap fraud since this is quite literally "where the money is". Successful SIM swap operations can make it easy for hackers to obtain things like verification codes and account information, giving criminals a discreet and simple entry point into a person's finances.

In order to prevent SIM Swap Fraud, Lusis provides an online, real-time transaction and authentication verification service. This is known as Lusis' SIM Swap Protection Service (Lusis SSPS).

Built within Lusis' Tango AI Fraud platform, Lusis SSPS gives the bank direct and immediate access to detect irregularities and protect clients, thereby stopping the immediate fraud action and, as a result, preventing multiple



fraudulent uses that would have occurred if the Sim swap hack had been successful.

Lusis SPS provides users of the service with SIM level information to inform if a SIM swap has recently occurred and to confirm that the mobile phone number and IMEI are consistent and owned by the known phone owner/user. A baseline of SIM data can be regularly compared against a SIM's current status, providing banks with an insight into level of risk a consumer has for having had their SIM swapped without their knowledge.

Lusis SSPS checks multiple variables to determine if a SIM has been swapped maliciously, relaying the resultant information to the bank, preventing the hacker from ever accessing any sensitive information or resources within the bank and elsewhere.

Meeting the Deadline-December2020

PSD2 states "Banks need to meet the deadline and be secure".

Lusis has a reputation for reliable, effective and rapid deployment of solutions. Lusis SSPS in no exception to this. In fact, we have made it very easy to onboard this service through existing channels already running Lusis' Tango platform. We have teamed up with a best in class global aggregator to enable banks to join the service and meet the PSD2 directive quickly and with minimal disruption.

Who is Lusis?

An international company, Lusis was incorporated in 1999 and provides Software for AI Fraud and Payment Systems. Based in France, UK and USA, Lusis provides software and services to all markets with particular strength within the global financial & payments industry built upon many years of experience in supporting clients in tackling the challenges of today's ever-changing world.

Lusis designs, develops, delivers and supports solutions that meet the diverse and ever-changing requirements demanded across the acquirer and issuer values chains. From online transaction processing, message switching and fraud monitoring through to loyalty programme deployment and cloud-based business services, the solutions deployed utilise Lusis' Tango platform foundation to align directly to the client's business process needs.

Uniquely, Lusis' solutions are not tied to any hardware set up or database. Our purpose is to enable business in a reliable, secure, low risk, high performant environment. Using micro-service architecture Lusis brings a wholly modern and truly flexible proposition and implementation to the Fraud and Payments Ecosystem. An appropriate payments vehicle for modern day businesses.

TANGO is easily configured to add more value to existing channel-specific services offered to customers and to respond rapidly to any new business opportunity that presents itself.

Please visit our website for more detail or contact us directly at: sales@lusispayments.com.

lusis Payments

France:

5 Cité Rougemont
75009 Paris
France
(+33) 1 55 33 09 00

United States Office:

315 Montgomery St.
#900
San Francisco, CA 94104
(+1) 415 829 4577

UK:

1 Northumberland Ave
Trafalgar Square
London, WC2N 5BW
(+44) 207 868 5288

Luxembourg:

321, route d'Arlon
L-8011 Strassen
Luxembourg
(+352) 31 35 02-1

www.lusispayments.com

sales@lusispayments.com