Financial Services Community Meeting #1
22.10.20

Questions answered by the experts

Question	Answer
Is there any data available how often SIM Swap fraud occurs?	It's a really good question. We haven't seen any globally published data and insight seems to be a country level. We will use the project to explore and confirm. Additional article resources: https://www.which.co.uk/news/2020/04/sim-swap-fraud-how-criminals-hijack-your-number-to-get-into-your-bank-accounts/ https://www.theguardian.com/money/2020/sep/13/sim-swap-is-on-the-rise-how-can-you-stop-it-happening-to-you
Does the API also cover the porting of a phone number from one carrier to another?	Good question. Yes ported-in numbers are defined as MSISDN-IMSI change and therefore we'll create a timestamp for these events within the service and API.
Do you have statistics how the SIM swap attack number decreased after the SIM swap API system had been deployed?	We don't have detailed data on this but general feedback from the banks, who are our customers, is very positive regarding reduction in successful SIM Swap attacks.
Did you noticed any activity prior to Sim Swap event occurred, like phishing calls or SMS?	Yes, but some of the attacks also just use research on social media to secure the credentials they needs.
What are the operators doing to verify the source of the SIM swap? Have operators considered user verification controls?	This differs dependant on which operator it is and what region. In general, we advocate for stronger verification controls ahead of sim swap to ensure it is the subscriber requesting. Some require secondary sources of ID others have a verification process based on pre-agreed shared secrets (pass phrase or similar).
Aside from Germany and Spain, where else will Telefonica be launching this API in the near future?	It's also available in Colombia and Ecuador from Telefonica, with other countries coming next year
Mobile carrier acct security was never set up with protection of a customers' life savings in mind. Are FinSvcs firms considering steps to lessen their reliance	Have they thought of it, yes, it is realistic to expect a significant change in SMS use, or indeed a delay like proposed, we would say not.

on SMS as a 2FA for transactions or to at least put a 24 hr or 48 hr delay for transactions confirmed via SMS?	
Do you look at any proactive data points that indicate a SIM Swap may be imminent and use these to increase security on the mobile account?	We tried to offer a really simple service that could be made available in a reasonable time by all operators and therefore focused only on timestamp, leaving the bank to use all the data points they had available to make the best risk decisions.
Do all the operators in UK follow specific standards to provide the SIM SWAP solution?	Yes, in UK we have more or less aligned around a standard approach, with some small differences between operators. More important though was to have the "timestamp" available than the actual specification being exactly the same.
Banks and Financial institutions are required to comply with security norms such as PCI-DSS / SWIFT security requirements etc. But it does not look like Telcos are required to comply with such standards. Is there sometime in the pipeline to formulate a global standard for Telcos to use?	There are several standards that operators conform to, most are around interoperability and core security standards, others are placed around the licensing terms for operating licenses (Usually country specific). James is currently speaking to the body of knowledge and recommendations available to telco around this topic. The GSMA and the operator community recognise this as an area that needs focus and resolution.
We have seen a number of threat actor groups recently using dual screen to 'watch' victims, where the user enters their 2FA on a fake site and the TA simply transposes that into the real web page. No SimSwap needed.	We hope through the community to address all key challenges. If you can share your insights with me directly then happy to explore how can explore and address.
In South Asia it is very common to have pre-paid MSISDNs / SIMs used for short term and then recycle the MSISDN. Any frauds do we know due to recycled MSISDNs?	It isn't a topic that we have seen reports on as relates to fraud - many operators that recycle numbers 'sleep' such for a period of time before re-issue. For fraud this process is not predictable and hence would be difficult to exploit. In UK Telefónica offers Recycle API service to allow SPs to determine change of ownership with a timestamp shared for last recycle/deactivation event. More info here: https://sandbox.smartdigits.io/apidocs/numberrecycle

How much direct communication with the financial community do you work with? is this a mobile only fraud and security group?	The GSMA Fraud and Security Group is currently a member lead group (Operators and associate members). Part of today is to start a broader communication with the financial services sector and be more inclusive.
Will the financial Group committee have representatives from Finance sectors such as individuals managing fraud and security of banks?	Yes, that is our goal. We would be delighted if more banks came to join this community.
Does the Financial Service Committee have members from Financial industry such as fraud and security members of banks?	The GSDMA Fraud and Security group has been focused on attacks on mobile operators- there are many. We are creating this forum to increase collaboration between mobile operators and banks. I am happy to discuss any thoughts you have on what might this work.

In which countries is this API available?	For Telefonica: UK, Spain, Germany, Colombia, Ecuador.
It was stated that hundreds of e-merchants have been compromised for e-skimming. Is there a list of those merchants and how was it determined their SW has been infected with e-skimmers?	There are analytical companies searching for that information who are ones who can elaborate the periodic lists with the compromised merchants. Most of those merchants are informed either directly or via Law Enforcement Agencies
SMS OTP scam is very rampant now, both via A2P and P2P. Most of the time, to make it look more legitimate these scammers uses Generic Sender Ids like infosms, verify, alert, notify etc... are there any list published globally for reference of what are the mostly used Generic sender ids?	We don't believe there is. We will look at SMS phishing in the New Year.
Concerning the SIM swap issue: Where do you see the largest potential to improve for the Telco's in Europe to tackle this kind of fraud in terms of processes or technology?	I know sure how to answer this question. It is more for the Telco's themselves to assess the vulnerabilities of the current system and what are the alternatives to make it safer
Has EUROPOL noticed a decline in SIM Swap based banking fraud activities after	No, we think it is still early to have a clear idea of the impact of the PSD2 in the levels of fraud. We will have to wait some more time to compare the situation before

the implementation of the PSD2 measures?	and after the PSD2. Additionally, there are also other factors that will condition it, not only the PSD2.
Does anyone have data on the value/cost of SIM SWAP fraud, either regionally or globally?	We haven't seen any published data Sham See Guardian article quoted above for cases and losses, but not prevented cases and losses
SIM Swap has a direct impact on payment and financial services. Do you have any suggestions or processes defined for integrating Telecommunication with the Banking industry?	We do believe there is an opportunity to work more closely together and welcome all contributions in this Community to make that happen.
Have you witnessed such SIM Swaps or account takeovers more when subscribers are in roaming? Is there any stat available that can show SIM Swap happening when subscribers are in a domestic network or more when they are roaming?	We don't have any insights on this, but we assume almost all SIM Swaps happen when subscribers are own home network
Financial Institutions like Citi have big teams to prevent Fraud. I heard a lot about collaboration with other MNO but I did not hear about collaboration with Banks. Is there ongoing collaboration with banks to prevent FRAUD?	UK MNOs and banks work closely, and we want to replicate that model through this community.
Not sure why a CFO would need to think about what project to push forward if there is a clear Business Case with Cost of Opportunity clearly valued. If the cost of opportunity is clear, then the decision is very clear	Noted.
Does silent number verification solve the SIM Swap problem for you?	Telefonica view: Silent Verification (or Number Verify) significantly enhances security in a number of ways (e.g., Malware SMS capture, social engineer SMS OTP capture) but we strongly recommend it to be deployed with a SIM Swap check to defend against account takeovers