PREVENTING MOBILE PHONE SIM SWAP FRAUD

Identity Verification is essential to the future of the online marketplace.
The exponential growth of the Digital Economy has created many challenges for business-es in validating and protecting their users' private information.These and other impediments such as establishing trust in the online marketplace and verifying users are costing business multiple billions annually and impacting consumer confidence.

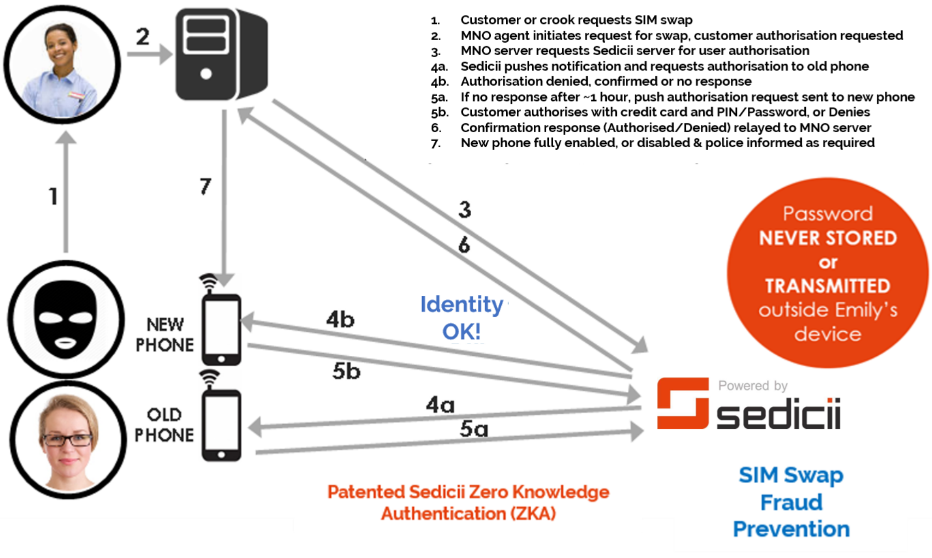
The threat of personal information: name, address, password, credit card details, etc. being regularly stolen for fraudulent use and monetary theft is constant and causing significant issues for all stakeholders of the digital economy. Consumer's credit cards can be used without their permission leading to their identity being exploited to create new accounts with online merchants for criminal activity.

Verizon Enterprise reported 53k+ security incidents, in its 2018 Data Breach investigations Report. Non-compliance with EU GDPR carries penalties of up to €20m or 4% of global revenue and this takes no account of the costs to business of the breach itself. Sedicii's unique ZKP technology helps organisations to comply with strict AML and Data Protection legislation as no data is exposed during the authentication process.

The Problem:

A fraudster obtains your bank account details and registers your mobile phone number through phishing or malware. He approaches your mobile service provider with your fake identity proof and, claiming loss of handset or SIM damage, seeks a duplicate SIM card. A SIM swap typically happens using the following methods: Using identity theft to convince a MNO shop assistant that they are dealing with the account holder; or by stealing passwords from employees at the mobile operators or mobile dealers. Bill pay cellular users' SIM cards can be cloned through a helpdesk by answering personal verification questions such as a home address or work number. The situation is more complex for pre-paid customers where the personal verification questions focus on the latest recharges or last numbers called. By using a fake ID document and other fake documents a person can also do a SIM swap at a mobile dealer. If a fraudster gains access (through a stolen password) to a support agent's account, or that of a mobile dealer assistant, the SIM swap process becomes easy. The SIM swap is typically performed late at night to avoid detection by the victim. Some fraudsters are also encouraging the victim to switch off their cell phone by harassing them with multiple calls. After the phone is switched off, they do the SIM swap without fear of detection. Some mobile operators send an SMS notification that a SIM swap has been requested. To avoid the SIM swap being stopped, the fraudsters either use the above method or call the victim masquerading as a mobile operator employee to tell them the SMS was sent by mistake and should be ignored. Following verification, the original SIM is deactivated and a new one is issued to the fraudster. He then initiates financial transactions from your bank account, details of which he had earlier stolen, and receives payment confirmation requests on the duplicate SIM. Since the original SIM has been deactivated, the real customer remains unaware of the fraudulent transactions being made on their account.

The Solu



1. Customer or crook requests SIM swap
2. MNO agent initiates request for swap, customer authorisation requested
3. MNO server requests Sedicii server for user authorisation
4a. Sedicii pushes notification and requests authorisation to old phone
4b. Authorisation denied, confirmed or no response
5a. If no response after ~1 hour, push authorisation request sent to new phone
5b. Customer authorises with credit card and PIN/Password, or Denies
6. Confirmation response (Authorised/Denied) relayed to MNO server
7. New phone fully enabled, or disabled & police informed as required

2
1
7
3
6
Identity OK!
4b
5b
4a
5a
NEW PHONE
OLD PHONE
Password NEVER STORED or TRANSMITTED outside Emily's device
Powered by sedicii
Patented Sedicii Zero Knowledge Authentication (ZKA)
SIM Swap Fraud Prevention

With Sedicii's Zero Knowledge Authentication (ZKA) the user's private PIN/password, IMEI, IMSI data is never sent outside the client device. Sedicii will *never* authorise a SIM swap without the express authorisation of the customer. If approval is not received, it is assumed the customer is unaware of the request and is immediately denied.

See Sedicii in Action...

A Sedicii demonstration can be arranged to experience the benefits of Sedicii Zero Knowledge Proof Verification in action.

To find about more or to set up a live demonstration, call or contact us using the details below.

Sedicii Headquarters
ArcLabs Research &
Innovation Centre,
W.I.T. West Campus,
Carriganore, Waterford
Ireland. X91 P20H
Phone: +353 (0)51 302191

Sedicii UK
Techhub
1-15 Clere St.
London
EC2A 4UY
Phone: +44 20 8144 8279

Sedicii USA
2F Plug and Play
Techcenter
440 N. Wolfe Rd.
Sunnyvale CA94086
Phone: +1 408 786 5485

Sedicii Tenerife
C/Fotografo Jose Norberto
Rodriquez Diaz Zenon, 2
Piso 3 Oficina 3-5
Tenerife 38204

Contact us online at:
Web: www.sedicii.com
Email:
contactus@sedicii.com
Twitter: @GRRSedicii

Sedicii has developed an out of band smartphone solution to help customers identify when a SIM swap is being requested so they can stop it before it happens in cases where the request has not been initiated by them. The Sedicii solution involves notifying the customer, via an out-of-band method, such as a push notification on their smartphone coming from the mobile operator’s app, that a SIM swap has been requested. If it is a genuine request the customer should authorise the change. If not, the request should be immediately denied.

Only when the customer has successfully authorised the SIM swap via the mobile operator’s app is the new SIM enabled. In the event that no response comes from the customer, the SIM will be provisionally enabled to allow it to be inserted in the new handset. The new handset/SIM combination must be registered with the mobile phone operator’s Sedicii server via their app. During this registration, the Sedicii server will detect a new IMEI and new IMSI. A push notification will be sent to the new handset asking for authorisation to fully enable the new combination. The customer will be asked to enter a combination of credentials e.g. their credit card details plus a PIN/Password which will be converted to a Sedicii signature and compared with a signature that was created at enrolment time. If the customer successfully authenticates the new phone will be fully enabled and the old one disabled. If not, the new SIM is disabled, police informed where required and the old phone re-enabled.

Sedicii employs multi factor, strong authentication solutions to increase security,
but not at the expense of convenience. In all the scenarios, the Sedicii service relies on the three factors of authentication “something you know, something you have, something you are” principle to prove that the user is the person who originally enrolled for a service. Identifiers are combined to generate a unique signature for the user/handset combination.

Commercial Considerations:

Sedicii can be deployed in an ‘on premise’ configuration on a licensed basis where the client enterprise will manage and maintain the service entirely independently. Or, it can be provided in a cloud configuration where the same service may be shared by a number of organisations or services. In this configuration, the service is delivered on a transaction basis and managed entirely by Sedicii on behalf of the client enterprises.

Sedicii proves that a customer is not being impersonated, quickly, securely and reliably, **WITHOUT** any underlying sensitive personal information having to change hands. The user’s identity attributes **NEVER** leave the device, browser or server. This reduces the burden of responsibility on the merchant whilst protecting the consumer. All sides win.