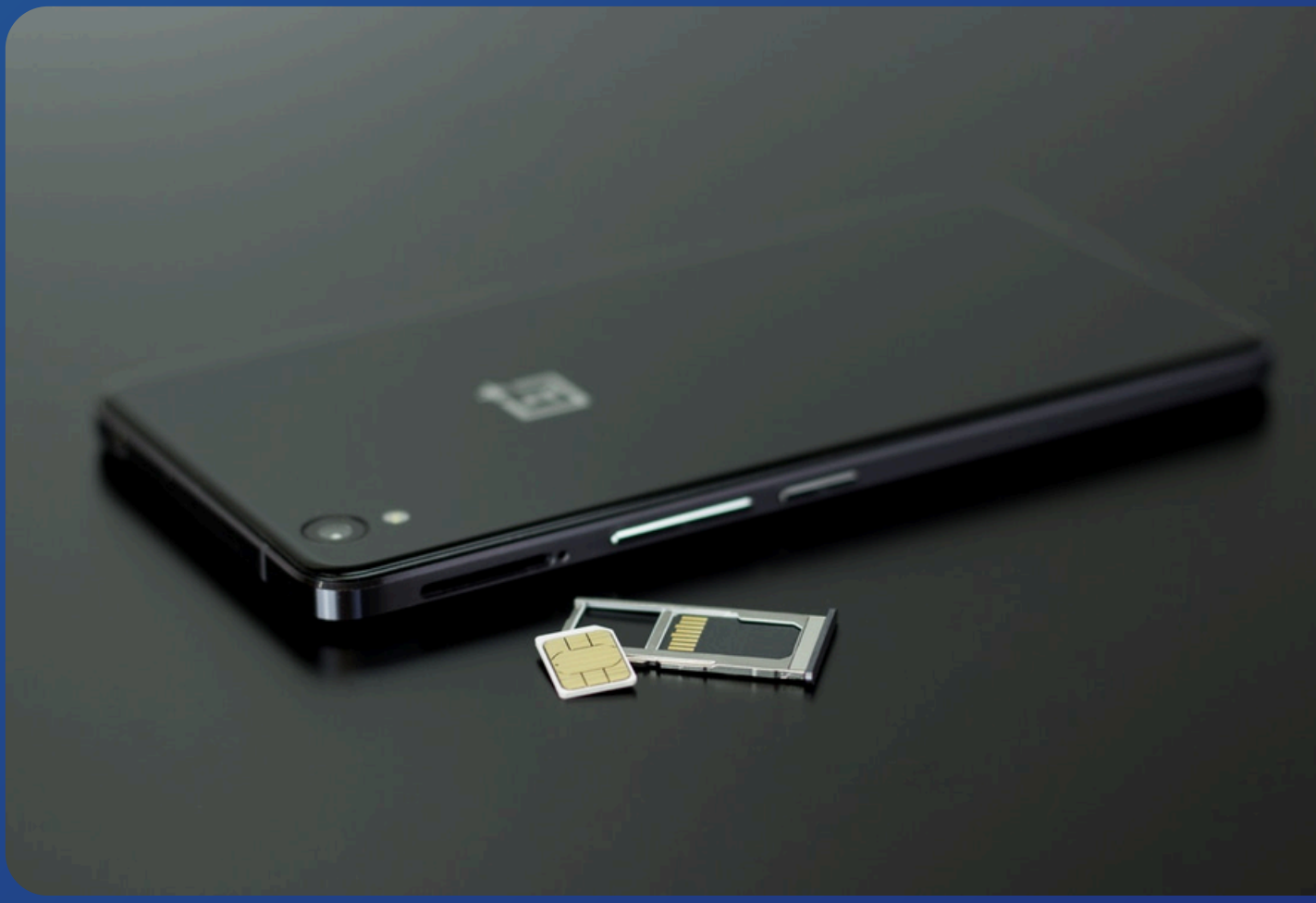
Whitepaper

PRIVACY LINKS

# THE RISE OF E-SIM SWAPPING

How the move to E-SIM brings new challenges in authentication fraud, leading to an explosive growth in SIM-swaps for Telcos.

www.privacylinks.eu



**The future is going to be E-SIM only.**

In 2035 it is expected that most new smartphones will no longer have a physical SIM card slot.

With 10% of current mobile connections going via E-SIM, forecasts show that 75% of connections will be purely E-SIM based in 2030.

With the move to more digital based SIM-activation, new avenues for fraud have arised that lead to a massive influx in SIM Swaps, identity theft & enterprise breaches.

This whitepaper explores the challenges in current E-SIM activation, the impact on Telco operations and the current solutions.

# Executive Summary

**The telecommunications sector faces an unprecedented threat from E-SIM swapping and social engineering attacks, with fraudulent SIM swaps surging 1,055% in 2024. This crisis threatens not only consumer & enterprise security, but also the fundamental business model and reputation of telecom operators.**

**With nearly 3,000 unauthorized SIM swaps reported in 2024 and £86.15 million in direct losses, the problem demands immediate action to protect both customers and business interests.**

Growth in Sim Swap Fraud

**1.055% in 2024**

With E-SIMS becoming the standard, UK SIM Swaps have risen by astounding amounts.

Direct sector losses in 2024

**€86.15 million**

GDPR fines & direct losses as a result of unsafe authentication & E-SIM activation systems have an impact on the bottom line.

Fraudsters are able to gather account information from customers & companies in a variety of ways. The most important tools being:

- **Spoofing**, acting as customers or telco-employees to gather trust, using e-mail or phone.
- **Social engineering**, gathering authentication information via calls and fake SMS's leading to duplicated webpages.

Core to the problem are unsafe communication channels between telco's & their customers and ineffective 2-factor authentication methods.

Lots of current 2FA systems hinder conversion and/or the ease of use for customers. Often not benefiting them besides additional safety. This leads to low adoption of safer alternatives, making the authentication & activation process prone to fraud.

PrivacyLinks offers a solution to authentication issues, whilst allowing Telco's to profit by offering customers & enterprise new value added services.

## Negative media coverage

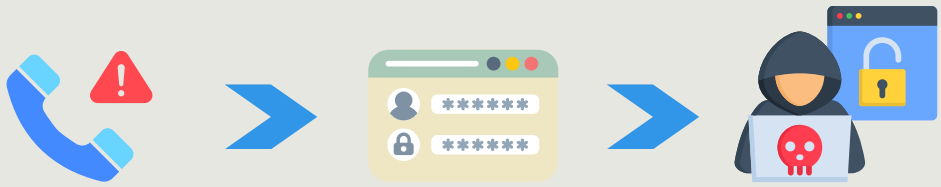
**Every swapped SIM and fine handed out leads to negative media coverage. With hacked customers spreading the word their Telco is not safe.**

**Damaging reputation, increasing churn and reducing NPS.**

# Key fraud techniques

E-SIM swapping is on the rise due to the absence of a hardware SIM. Fraudsters gain access to accounts of customers in multiple ways, allowing them to swap SIMs and do undesired transactions, leading to high costs, identity fraud and more.

## Social Engineering

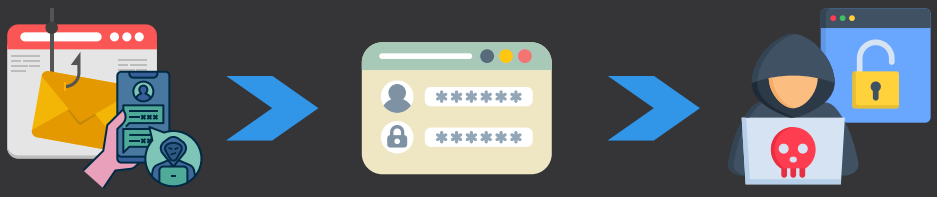



Fraudster calls customer, pretending to be Telco-employee

Convinces customer to give login-details & 2FA-code

Gains access to account & swaps SIM / does transactions

## Smishing & Phishing




Fraudster sends fake e-mail or SMS with link for account recovery or E-SIM

Customer lands on spoofed webpage & tries to login

Fraudster simultaneously logs in to real Telco-portal, gaining access

## Activation code interception


Customer receives E-SIM QR activation code in e-mail

Fraudster has access to mailbox & loads E-SIM to their phone

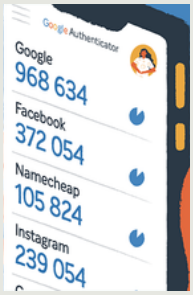
Can recover victim's passwords & account credentials via SMS-2FA

# The Challenge:

E-SIM fraud is a result of unsafe authentication systems. Existing systems are prone to Social Engineering attacks of fraudsters and offer no additional benefit to customers.

# Current solutions are ineffective

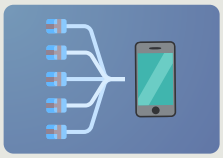

SMS or E-mail based 2FA codes are common, but prone to Social Engineering due to their shareable nature.




Authenticators require customers to perform more steps, are just as unsafe as SMS-2FA and offer no additional benefit.

Spoofing & phishing filters only reduce the amount of phishing attempts, but are not 100% foolproof.

# Key vulnerabilities:



**Anyone can reach existing communication channels such as phone numbers and e-mail of customers, facilitating spoofing & phishing.**

**Customers can unknowingly share login details, 2FA codes & E-SIM activations with third parties. Facilitating social engineering.**

**Current solutions such as authenticators offer no benefit to customers and instill conversion barriers. Hindering adoption.**

# The business case for action

Countering E-SIM swapping is detrimental for ensuring quality service to consumers and enterprise alike. Failing to meet standards, leads to a loss of revenue and corporate image.

## Telcos are held responsible for fraud

GDPR bodies crack down on unsafe systems with fines

Customers churn as they lose trust in their telco

Negative media impacts the long term brand image

## Staying ahead of the threat

By implementing new solutions, telcos can stay ahead of the threat and strengthen their service they are offering. Simultaneously, new solutions offer a broad scope of new revenue models and value added services to consumers and enterprise customers.

PrivacyLinks specializes in solving urgent matters in authentication and communication fraud, while offering telcos new revenue opportunities in the slipstream.

## Keen on discovering solutions?

Contact us for strategic advise and to discover how to solve problems with E-SIM swapping by turning a problem into a profitable opportunity.

**Joes@privacylinks.eu**
**+31642024418**

# Our Team

**Tijn Kooijmans**
CEO/CTO

**Jurrie Christians**
CCO

**Joes van Stralen**
CMO

Kabisa
Software Artisans



**Rotterdam** – Frame Offices
Karl Weisbardstraat 181
3015 GM, The Netherlands

info@privacylinks.eu
+31 (0) 85 04 08 013