IMAGEWARE SYSTEMS

SIM Swap Fraud: A Global Epidemic

2FA is the Solution that Became the Problem

> "We identified flawed policies at 5 U.S. mobile carriers that enable straightforward SIM swap attacks."[1]

WHAT IS SIM SWAP?

Criminals use bribes, phishing, social engineering, and other tactics to get carriers to provide access to subscribers' phone numbers, allowing them to bypass SMS and 2FA.

THE SOLUTION:

The only way to fully mitigate the risk of SIM swap and other identity-related attacks is to rely on biometrics. Combining unmatched security with ease of use, biometrics authentication protected by advanced anti-spoofing is the unrivaled choice for secure and easy user verification.

2FA HAS BEEN EXPOSED IN THE NEWS

18-year-old hacker stole crypto worth $50 million in SIM-swapping scam.

Judge denies AT&T request for dismissal in the $224M SIM swap crypto case.

Twitter CEO Jack Dorsey's account hack exemplifies the simplicity of SIM swap.

HARSH REGULATORY FINES

EU (GDPR) can impose fines up to 4% of annual revenue and have already fined multiple companies for millions of dollars.

The U.S., through individual state legislation such as CCPA, is expected to be even more financially stern.

FRAGILE PROTECTION

2FA is not only subject to SIM swap attacks but numerous other hacks such as man-in-the-middle and phishing attacks.

> "SMS [authentication] is deprecated and will no longer be allowed."[2]

For more information call **(858) 673 8600**
or email **sales@iwsinc.com**

[1] "An Empirical Study of Wireless Carrier Authentication for SIM Swaps" — Princeton University (2020)

[2] NIST Digital Authentication Guideline (2016)