Strong Customer Authentication

16 September 2019

EBA opinion on the elements of Strong Customer Authentication

SCA is an authentication method based on the use of two or more elements categorized as possession *(something only the user possesses)*, knowledge *(something only the user knows)* and inherence *(something the user is)* that are independent, so the breach of one does not compromise the reliability of the others, and is designed in a way to protect the confidentiality of the authentication data

Something only the user own

Possession elements	*SCA Compliant**
Possession of a device evidenced by an OTP generated by, or received on, a device *(hardware or software token generator, SMS OTP)*	✓
Possession of a device evidenced by a signature generated by a device *(hardware or software token)*	✓
Card or device evidenced through a QR code (or photo TAN) scanned from an external device	✓
App or browser with possession evidenced by device binding — such as through a security chip embedded into a device or private key linking an app to a device, or the registration of the web browser linking a browser to a device	✓
Card evidenced by a card reader	✓
Card with possession evidenced by a dynamic card security code	✓
App installed on the device	✗
Card with possession evidenced by card details *(printed on the card)*	✗
Card with possession evidenced by a printed element *(such as an OTP list)*	✗

Something only the user knows

Knowledge elements	*SCA Compliant**
Password	✓
PIN	✓
Knowledge-based challenge questions	✓
Passphrase	✓
Memorized swiping path	✓
Email address or user name	✗
Card details *(printed on the card)*	✗
OTP generated by, or received on, a device *(hardware or software token generator, SMS OTP…)*	✗

Something the user is

Inherence elements	*SCA Compliant**
Fingerprint scanning	✓
Voice recognition	✓
Vein recognition	✓
Hand and face geometry	✓
Retina and iris scanning	✓
Keystroke dynamics	✓
Heart rate or other body movement pattern identifying that the PSU is the PSU *(e.g. for wearable devices)*	✓
The angle at which the device is held	✓
Information transmitted using a communication protocol, such as EMV® 3-D Secure	✗
Memorised swiping path	✗

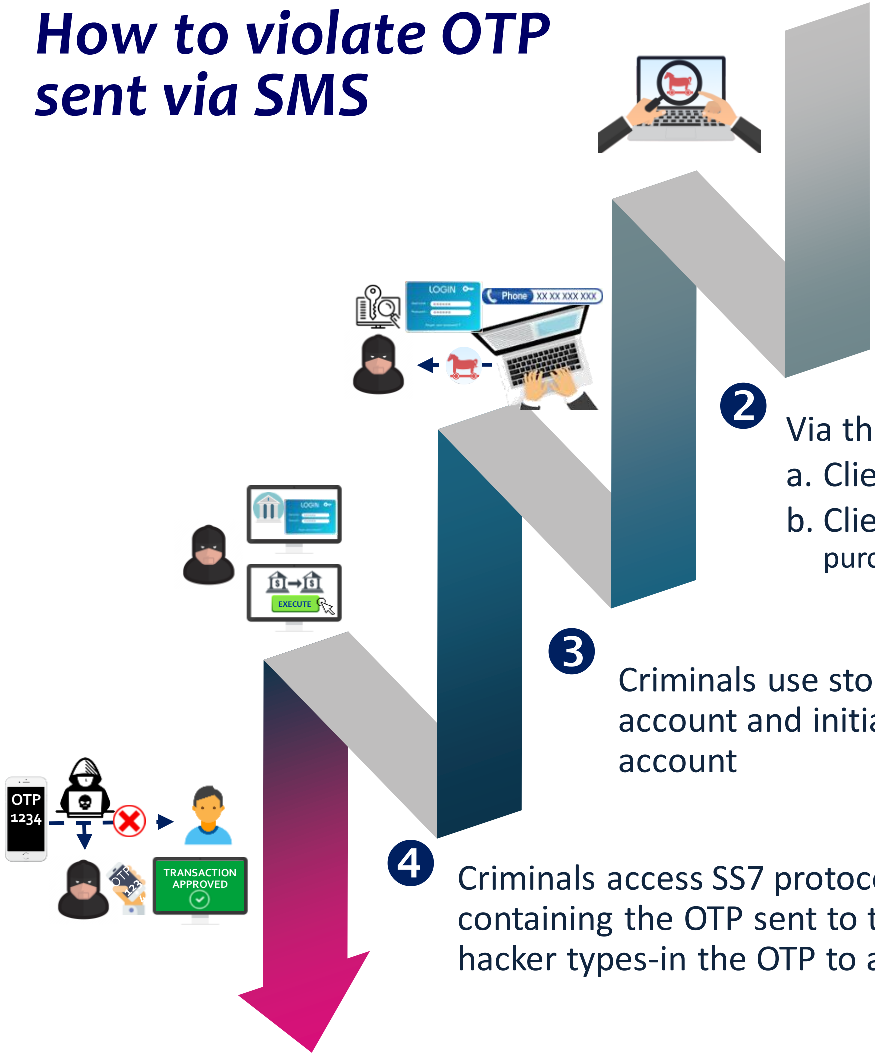
Source: EBA-Op-2019-06, 21 june 2019

Compliance with SCA requirements is dependent on the specific approach used in the implementation of the elements.

The most popular SCA process – based on OTP via sms – has been already violated

Cybercriminals have recently concentrated their efforts in violating a popular SCA process and were successful:

How to violate OTP sent via SMS



❶ Client PC is infected by a Trojan virus.

Hacker gets to see the client's logs related to his online sessions

❷ Via the Trojan hackers get to know:

a. Client bank account credentials

b. Client mobile number (often requested when purchasing online)

❸ Criminals use stolen credentials to access the client bank account and initiate a money transfer to their own account

❹ Criminals access SS7 protocol on behalf of a foreign carrier and forward SMS containing the OTP sent to the client mobile number, to their own phone. Then hacker types-in the OTP to authorize the money transfer

- Exploited flaws in SS7 telecom protocol to route to their own phone texts messages sent for 2-factor-authentication
- Cases of violation of the SS7 protocol have been reported recently by UK and German banks

O2 A Telefónica company   Metrobank

PSP Requirements to apply SCA exemptions

Article 16 of the RTS mandates the PSP requirements to apply SCA exemptions

Art.16 (b)

Real time fraud monitoring needs to be implemented. This is in addition to Article 2 which mandates that all PSPs must carry out some form of transaction monitoring

Art.16 (e)

Fraud audits and reports need to be developed and made available to the competent authority

Art.16 (f)

Fraud calculation approach documentation needs to be made available to the competent authority

Art.16 (g)

Notification to the competent authority is required if a PSP intends to use this exemption

In addition, if a PSP's fraud levels rise above the €100, 0.13% rate for 2 consecutive quarters they cannot use the exemption, and must alert the competent authorities

Considerations for acquirers when offering Art. 16's exemptions to merchants

Transactions will be covered by the liability shift principles of PSD2 Art. 74(2) where the acquirer is responsible for transaction losses where no SCA is applied. However only the acquirer can exempt transactions from SCA, **not** the **merchant**

The issuer may still apply SCA where it has identified a "materially increased risk of fraud" (Comments 53 & 85, Art. 18(5)). In this case the transaction is declined (ideally providing the appropriate decline code) and the merchant would need to re-try

Recommended actions for PSPs going forward…

- Many PSPs need to act toward **lowering** their **fraud levels** below the € 100 threshold, particularly through investments in real time fraud monitoring
- Also Art. 16 creates **opportunities** for acquirers to offer new risk based SCA **exemption services** to merchants. *(Not ideal – as also merchants should have this option – but moving in the right direction)*

Source: EBA

Merchants involvement in authentication risk assessment reduces transactional risk

Including the merchant’s customer knowledge in the transaction risk analysis improves accuracy of the assessment risk

- The consumer spends much more time browsing the merchant's web pages than at checkout
- Longer time spent at browsing implies a greater ability to collect customer data, useful in profiling customer behavior
- In addition, the data available to the merchants complement customer data available to issuer and acquirer: their combination allow to build an accurate customer profile that improves over time and create a high barrier to fraudsters as it is a moving target

Merchant data collection

Mouse dynamics, browsing behavior, shopping behavior…….

Issuer data collection

Keystroke dynamics of recurrent types *(eg. payment instrument)*, customer device, location…….

CleverAdvice
Via Ferrante Aporti 34
20125 Milano, Italy

T +39 02 39660672
F +39 02 2870768

e postmaster@cleveradvice.eu
w cleveradvice.eu

Results not Reports