twilio

PSD2, SCA, WTF?

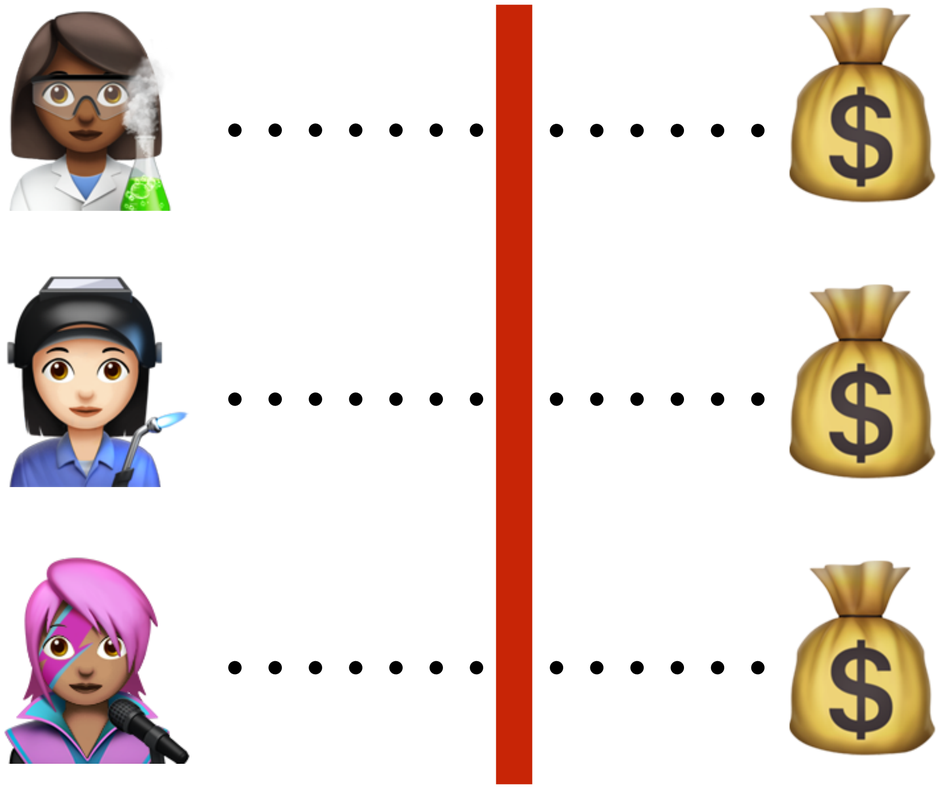
What to expect from the EU legislation

Kelley Robinson

@kelleyrobinson

Assumptions

1. Your users have something of value connected to an account

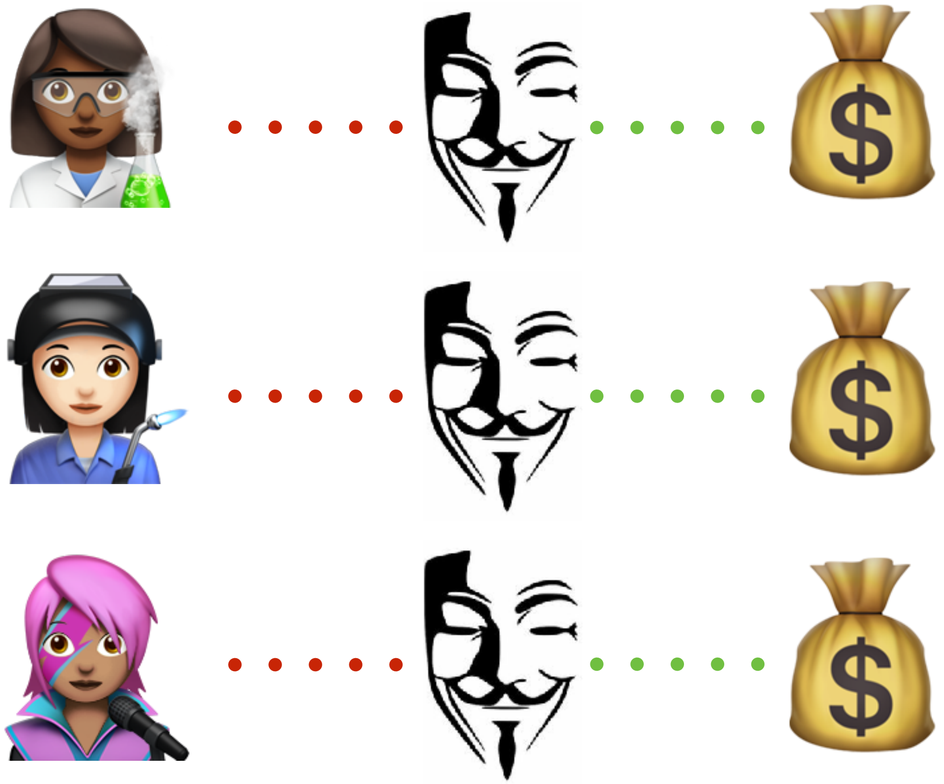


Assumptions

2. A user can only access the value once they are authenticated

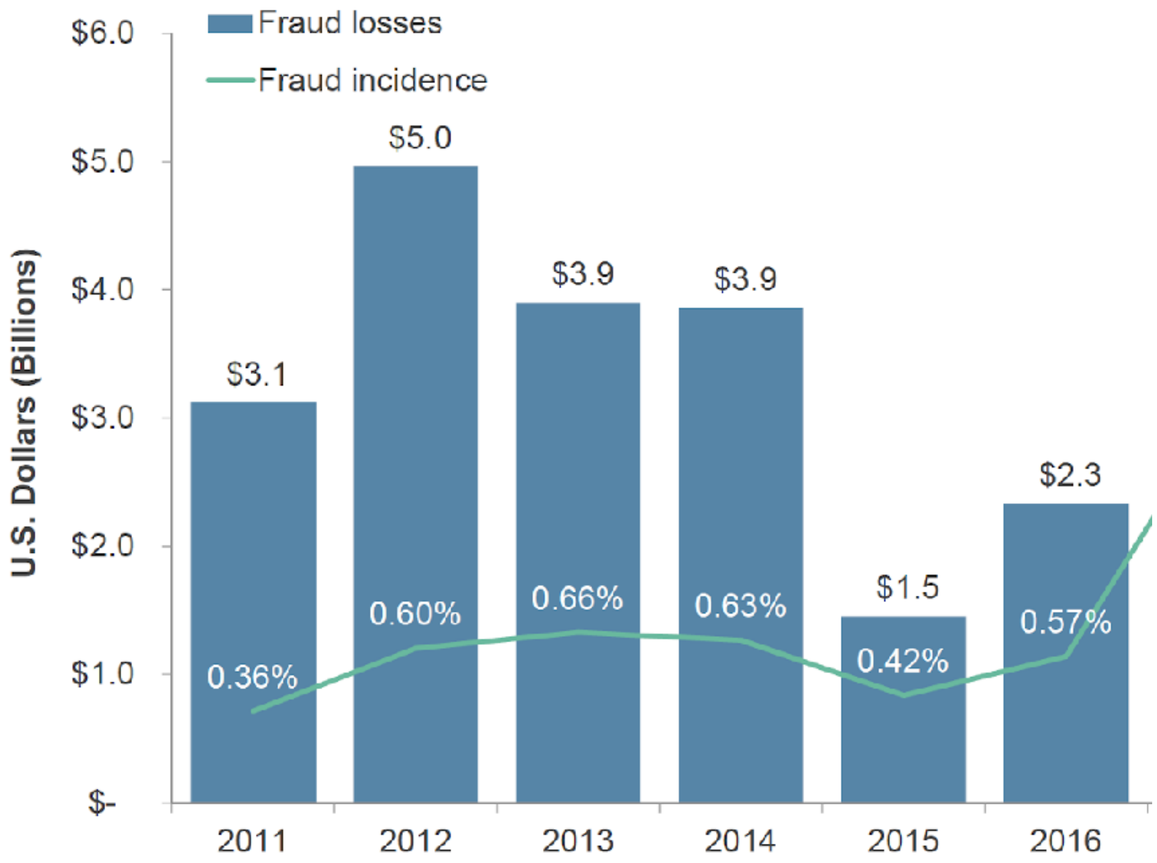
Assumptions

3. A successful impersonator could also access that value



Account Takeover Fraud Hits Record High, Nearly Triples in 12 Months

Figure 13: Account Takeover Fraud Incidence Rate and Dollar Amount of Losses, 2011–2017

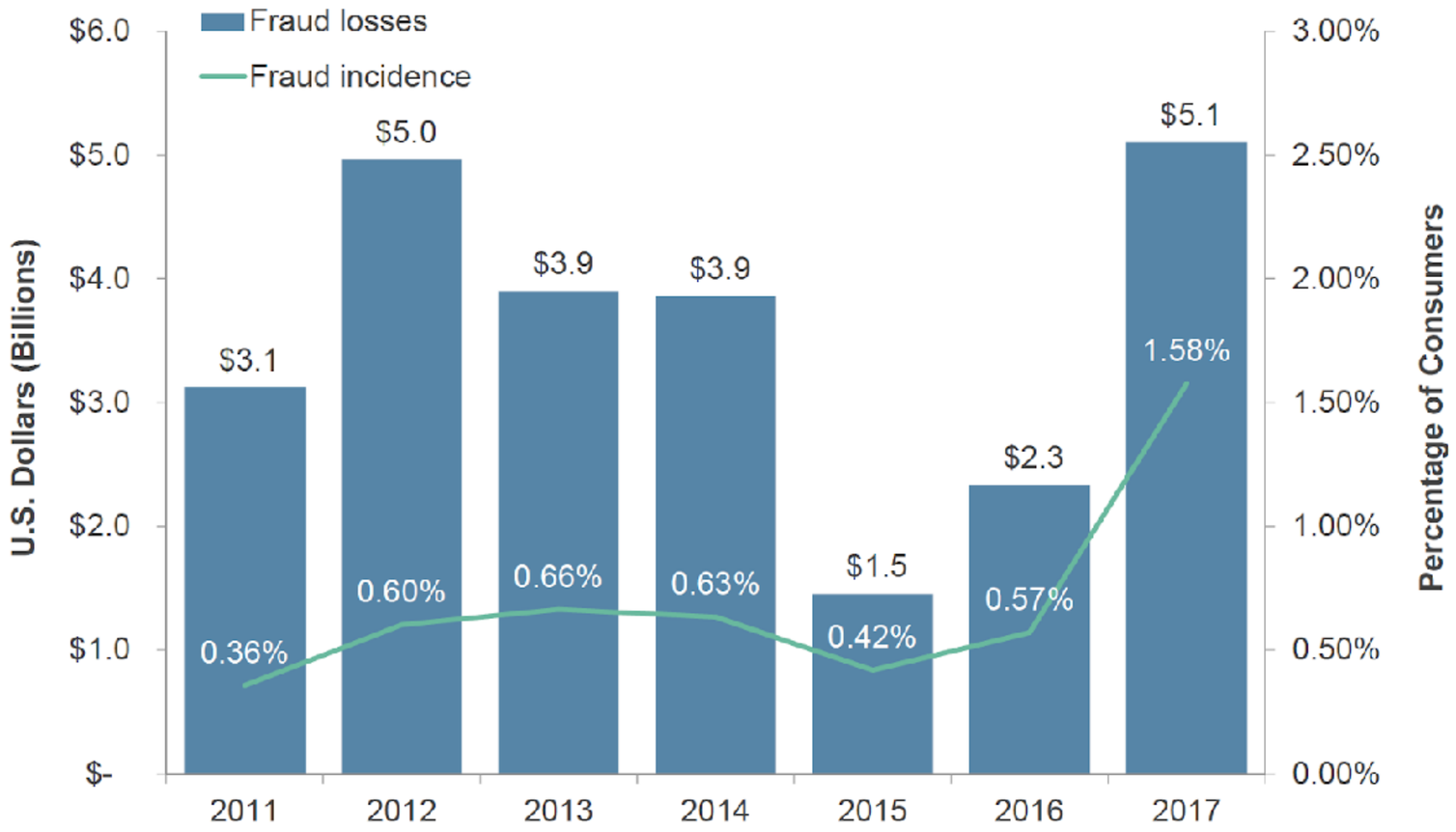


Source: Javelin Strategy & Research, 2018

How common is this?

Account Takeover Fraud Hits Record High, Nearly Triples in 12 Months

Figure 13: Account Takeover Fraud Incidence Rate and Dollar Amount of Losses, 2011–2017



Source: Javelin Strategy & Research, 2018

💰 $5.1B 💰

In 2017

PSD2

Payment Services Directive 2

The original PSD (2007)

- Objective: create a single market for modern payment services in the EU
- Add consumer protections
- Paved the way for new payment disruptors

What is PSD2? (2015)

- Updated regulations governing payment service providers in the European Union
- Applies to card not present (online) transactions
- Increase safety of cross-border payments

What's new in 2019?

Strong customer authentication (SCA)

for **all purchases over €30**

Scenarios where SCA applies:

The payer...

A Accesses its payment account online

B Initiates an electronic payment transaction

C Carries out any [risky] action through a remote channel

AUTHENTICATION FACTORS

Two are required to achieve SCA

INHERENCE

BIOMETRIC

POSSESSION

MOBILE PHONE

KNOWLEDGE

PASSWORD


PREMIUM Credit

Beginning **14 September 2019**, non-compliant payments that require SCA will be **declined**.

Dynamic Linking Explained

Dynamic Linking Explained

- Each transaction must have a **unique authentication code**
- Specific to the **transaction amount** and **recipient**
- Both amount and recipient are **shown to payer**

Use code 312568 to approve your Flourish and Blotts transaction of €713.00 to Gilderoy Lockhart

Dynamic Linking Security Requirements

(a) the payer is made aware of the amount of the payment transaction and of the payee;

(a) the payer is made aware of the amount of the payment transaction and of the payee;

Ensure the **user is confident** they are **authenticating the right transaction.**

(b) the authentication code generated is specific to the amount of the payment transaction and the payee agreed to by the payer when initiating the transaction;

(b) the authentication code generated is specific to the amount of the payment transaction

Any code must be used for
that specific transaction only.

(c) the authentication code accepted by the payment service provider corresponds to the original specific amount of the payment transaction and to the identity of the payee agreed to by the payer;

(c) the authentication code accepted by the payment service provider corresponds to the original specific amount

Once a valid code is accepted, **other channel codes are invalidated.**

(d) any change to the amount or the payee results in the invalidation of the authentication code generated.

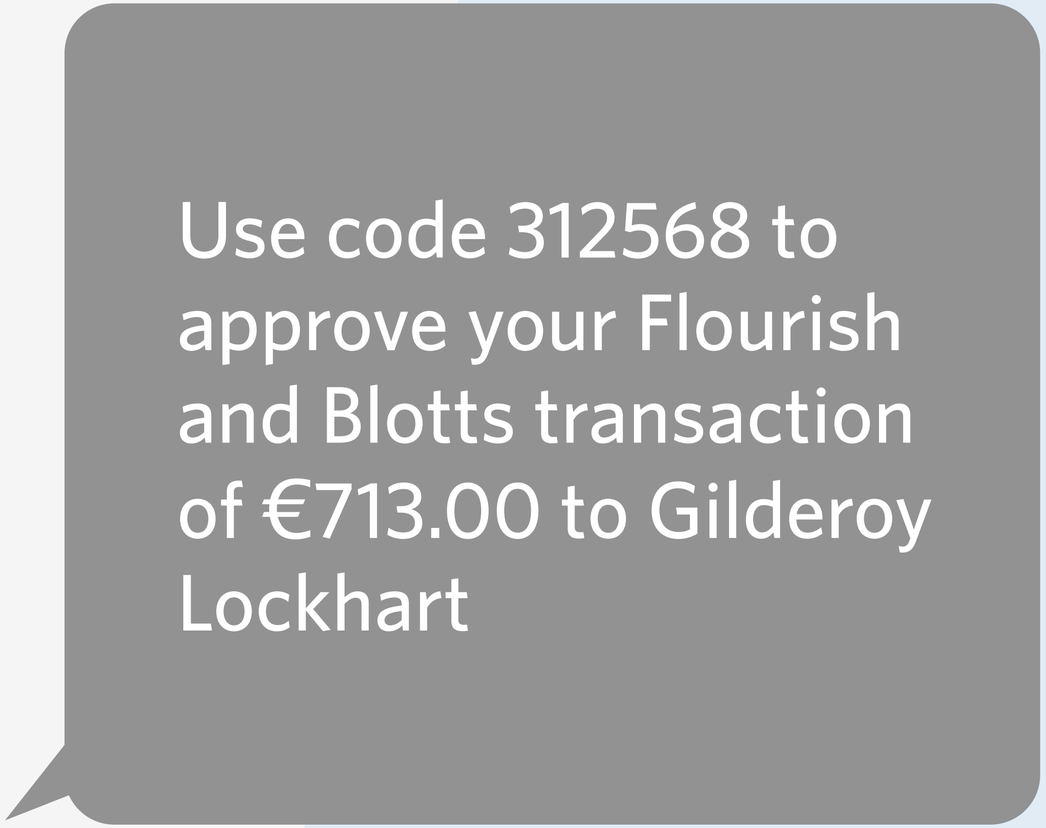
(d) any change to the amount or the payee results in the invalidation of the authentication code generated.

If transaction details change, **invalidate all outstanding codes.**

How to Implement SCA

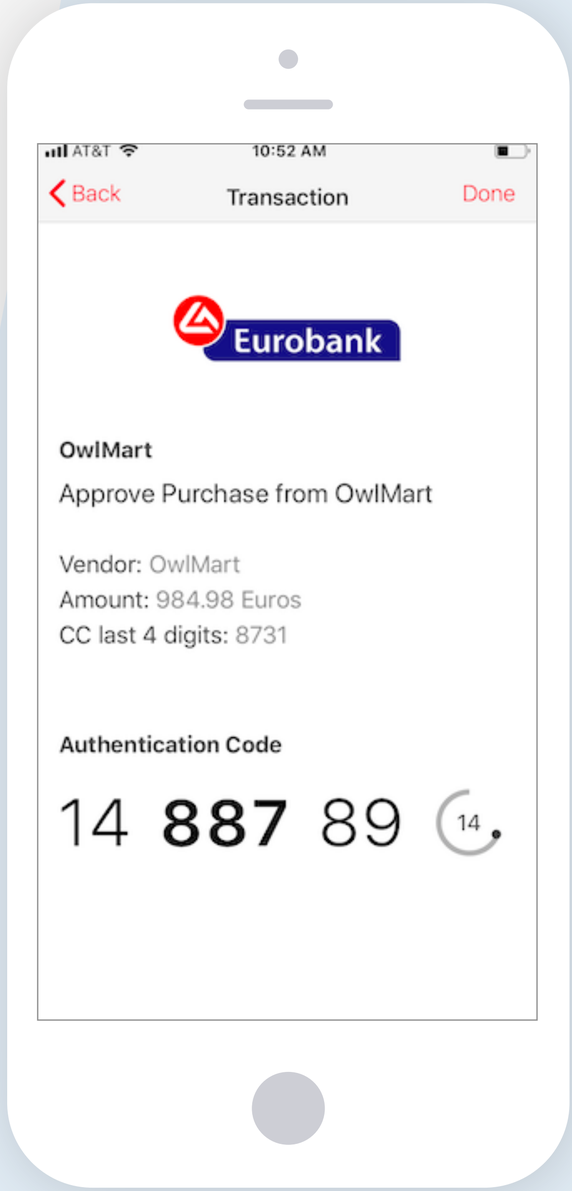
SMS

- No app install required
- Easily include transaction info in the message body
- Vulnerable to phishing & man in the middle attacks



Transactional TOTP

- Requires Authy
- Works offline
- Based on the Time-based One-time Passwords RFC 6238 standard
- More secure than SMS



Push Authorization

- Requires a special app (or SDK + dev work)
- Cryptographically most secure
- Seamless user experience
- Easily customize with your brand

Research groups **recommend push-based authentication over SMS** because of the secure connection between the retailer, the 2FA service, and the device, **removing opportunities for phishing.**

Security = Friction

Friction = Abandoned carts

Time is money

- Slow transactions may lead to fewer sales
- Offer options (+retries) to keep customers happy

What next?

- Are you a payment service provider?
- Does your PSP already provide a solution?
- Do you need to build your own solution?

Resources

About PSD2 + SCA

Understanding Dynamic Linking

Twilio PSD2 E-Book

Stripe's Guide to SCA

McKinsey Report on PSD2

Wikipedia PSD Reference

Implementing SCA

Twilio Documentation

Transactional TOTP Guide

Push, SMS Guide with Twilio + Python

THANK YOU

@kelleyrobinson