

Trending: Mobile Payments

- Dan McLoughlin, VASCO Data Security
- Julian Sawyer, Starling Bank



Trending: Mobile Payments

Dan McLoughlin, VASCO Data Security

Finextra

ABE  EBA
EURO BANKING ASSOCIATION



Can banks provide a **frictionless** consumer experience via **mobile wallets** without sacrificing **strong authentication** and **security** in **mobile payments**?

Dan McLoughlin

PSD2 Requirements for Mobile Wallets



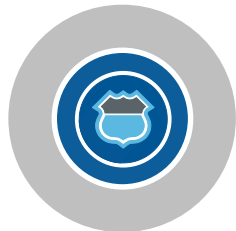
Multifactor Authentication Platform
to ensure compliancy with reliability and independence of authentication elements



Dynamic linking with secure channel technologies
to ensure CIA compliancy through **all** phases of payment authentication



Secure provisioning of personalized credentials
to mitigate risks of unauthorized use



Mechanisms to prevent and detect alteration of mobile apps
to mitigate risks of mobile device being compromised

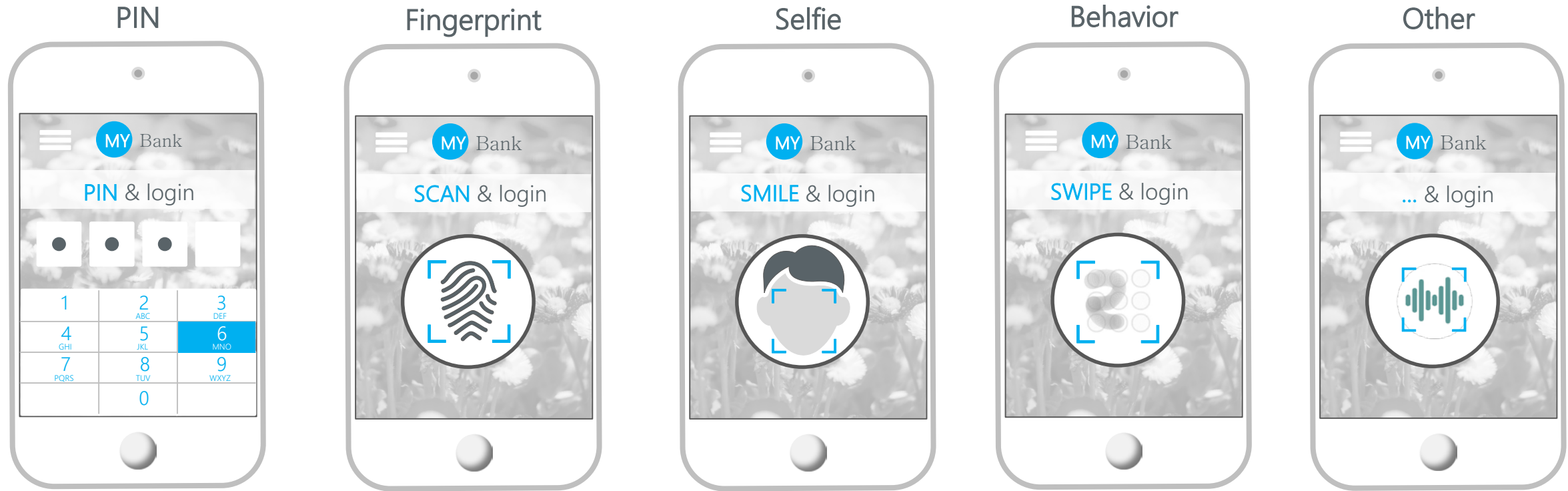


Fraud & Risk Manager
to comply with transaction monitoring and risk analysis requirements

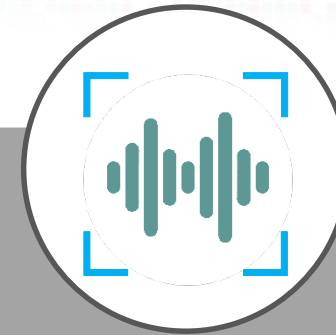
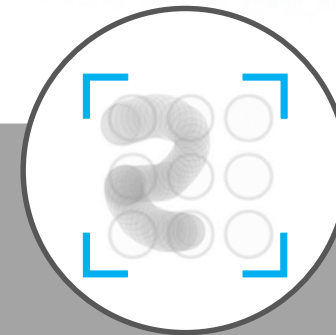
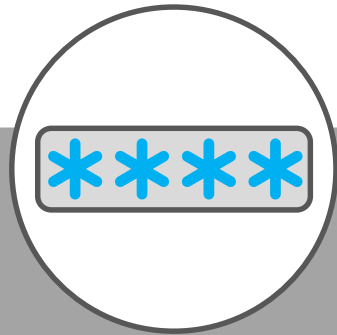
European Banking Authority's difficult trade-offs between competing objectives of PSD2



Strong Customer Authentication Options



VASCO Multimodal Biometrics Platform



User-Facing technologies

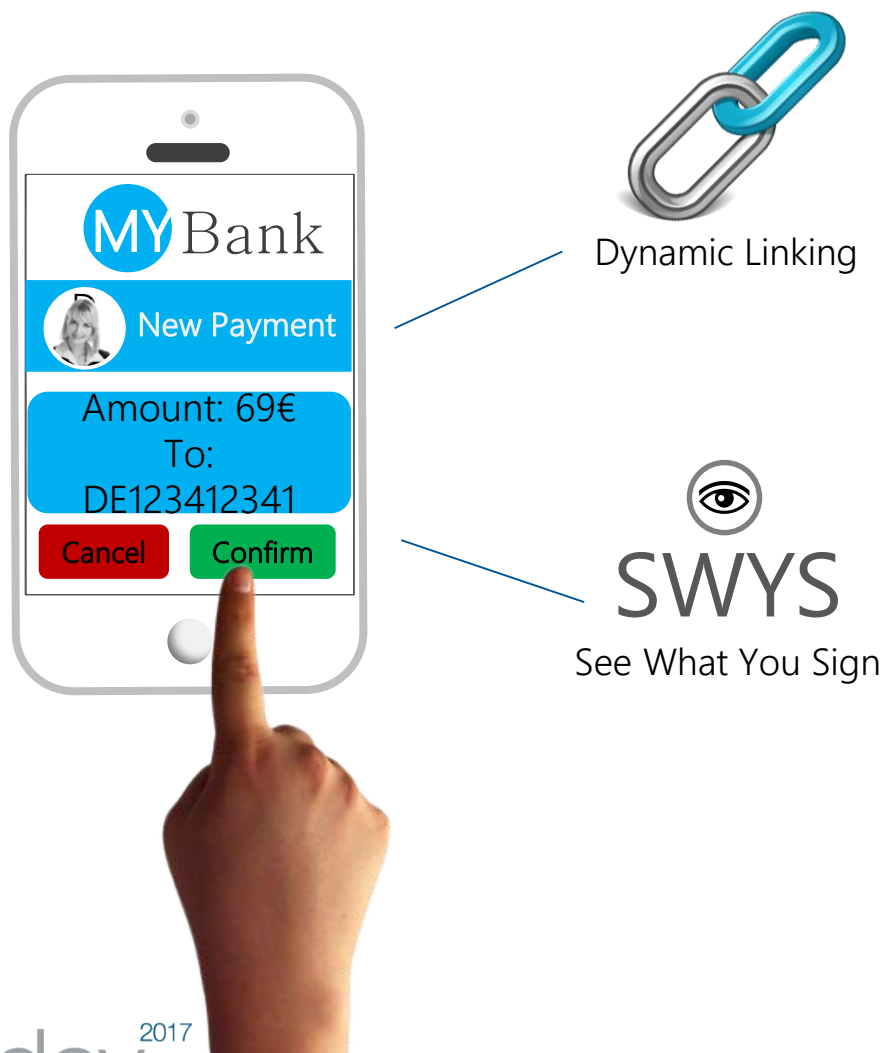
VASCO's Underlying Security Framework

Biometric
result

Multi-factor
Authentication code

Device & User
Contextual Data

Requirements related to transaction authentication



Authentication code is linked to the amount and the payee

Ensuring CIA of the amount and the payee through ALL phases of authentication

The payer is made aware of the amount and of the payee

Ensuring CIA of the information displayed to the payer through ALL phases of authentication

Touch & Check

Device & User
Contextual Data
+
Authentication Code
automatically sent

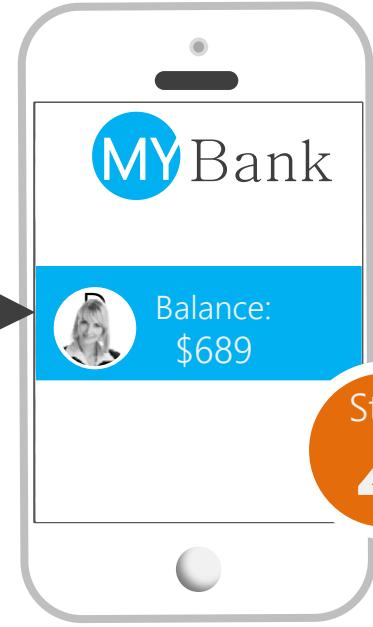
Step 1
User
opens the app
on trusted device



Step 2



Step 3
Transparent authentication



Step 4

Trusted device
shows balance &
recent transactions

Behavioral Biometrics



Behavioral biometrics provide evolving cross-channel and cross-platform identity recognition for continuous authentication and detect full scale fraud attempts (e.g. bot activities)

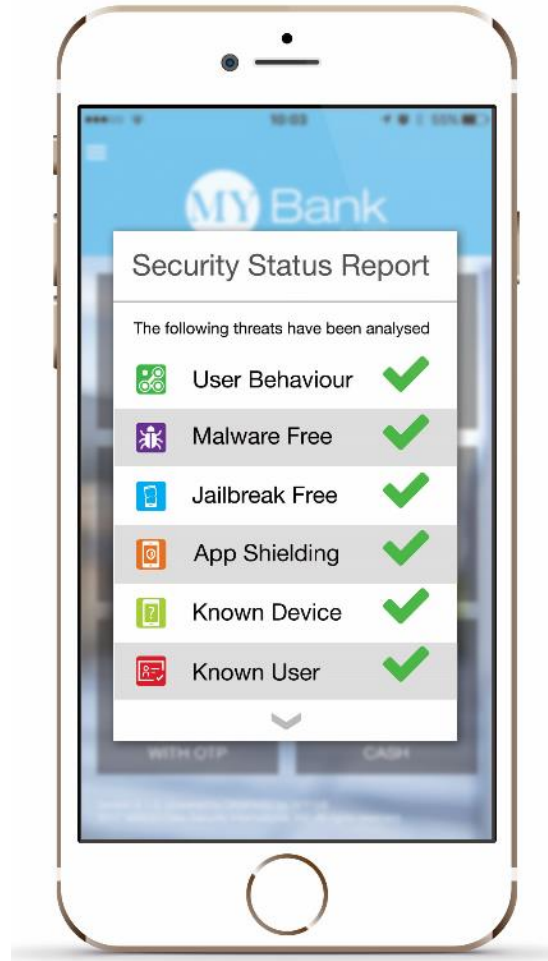
Data Points:

- Keystroke Dynamics
- Pressure
- Gyroscope
- Button hit zone
- Surface
- Motion
- Accelerometer
- Mouse
- ...

Runtime Application Self-Protection (RASP)

RASP is a set of technologies used to add security functionality directly to mobile applications for the detection and prevention of application-level intrusions

Anti Debugger
Anti Emulator
Anti Repackaging
Tamper Detection
Anti Code Injection
Removal Protection
Anti Key logging
Obfuscation
Active Memory Zeroing
Anti Screen Reader
Anti Screenshot
Anti Screen Mirroring
Lock external display
Lock Copy/Cut/Paste



PROTECT

Code obfuscation

DETECT

Ensure app is running in safe environment

- Debugger
- Emulator
- Jailbreak / Root detection
- Keylogging
- Screen reading

Ensure app is not altered or tampered

- Repackaging detection
- Resource verification
- Hook detection

REACT

Screenshot detection / blocking

Blocking external screens

Custom reactions

Alert / reporting

Shutdown (Exit / Fail)

Strong dynamic linking with Notification

Device protected against cloning and compromise

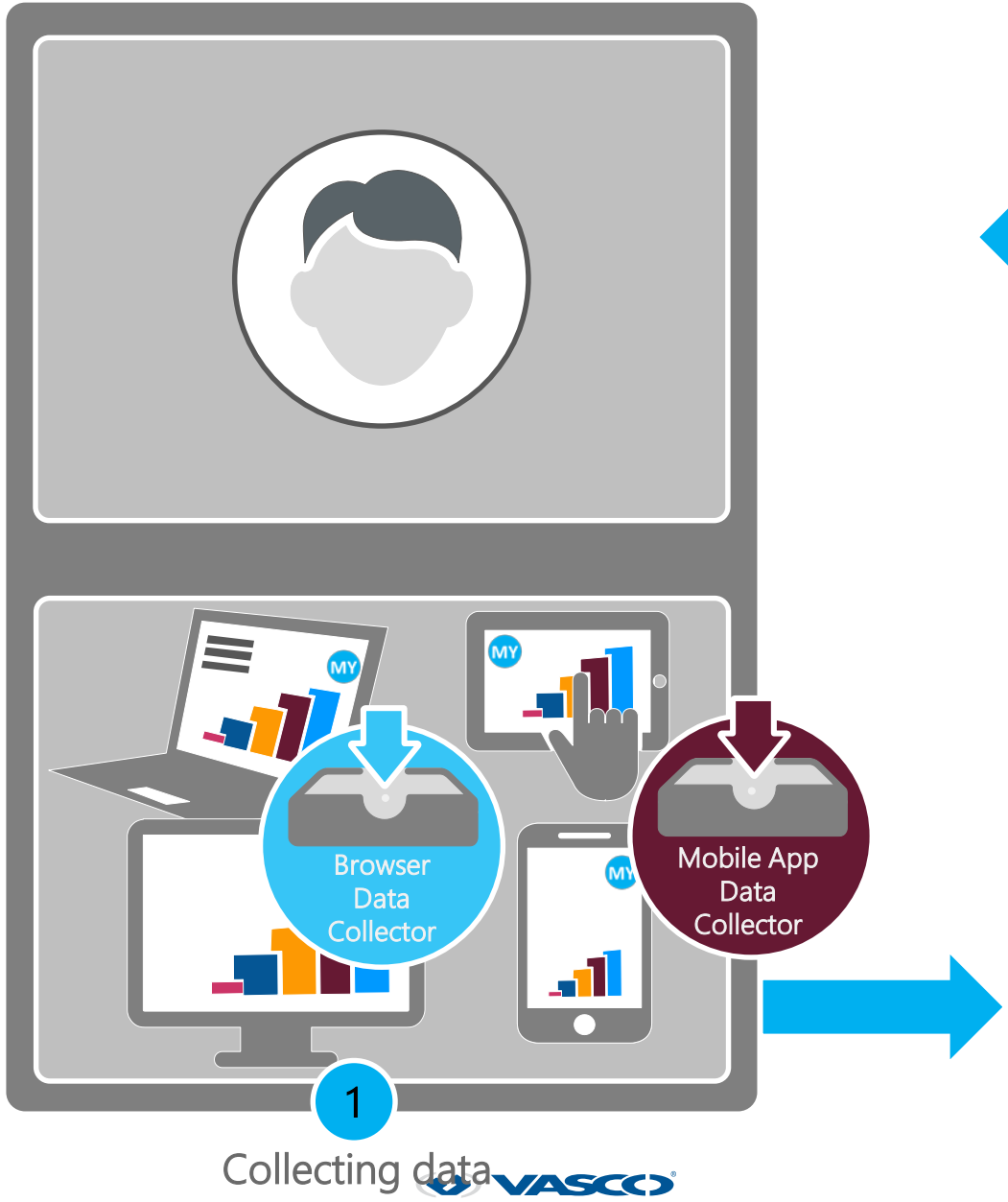
Notification is linked to encrypted transaction

User is **always** aware

Enhanced **SWYS**
See What You Sign

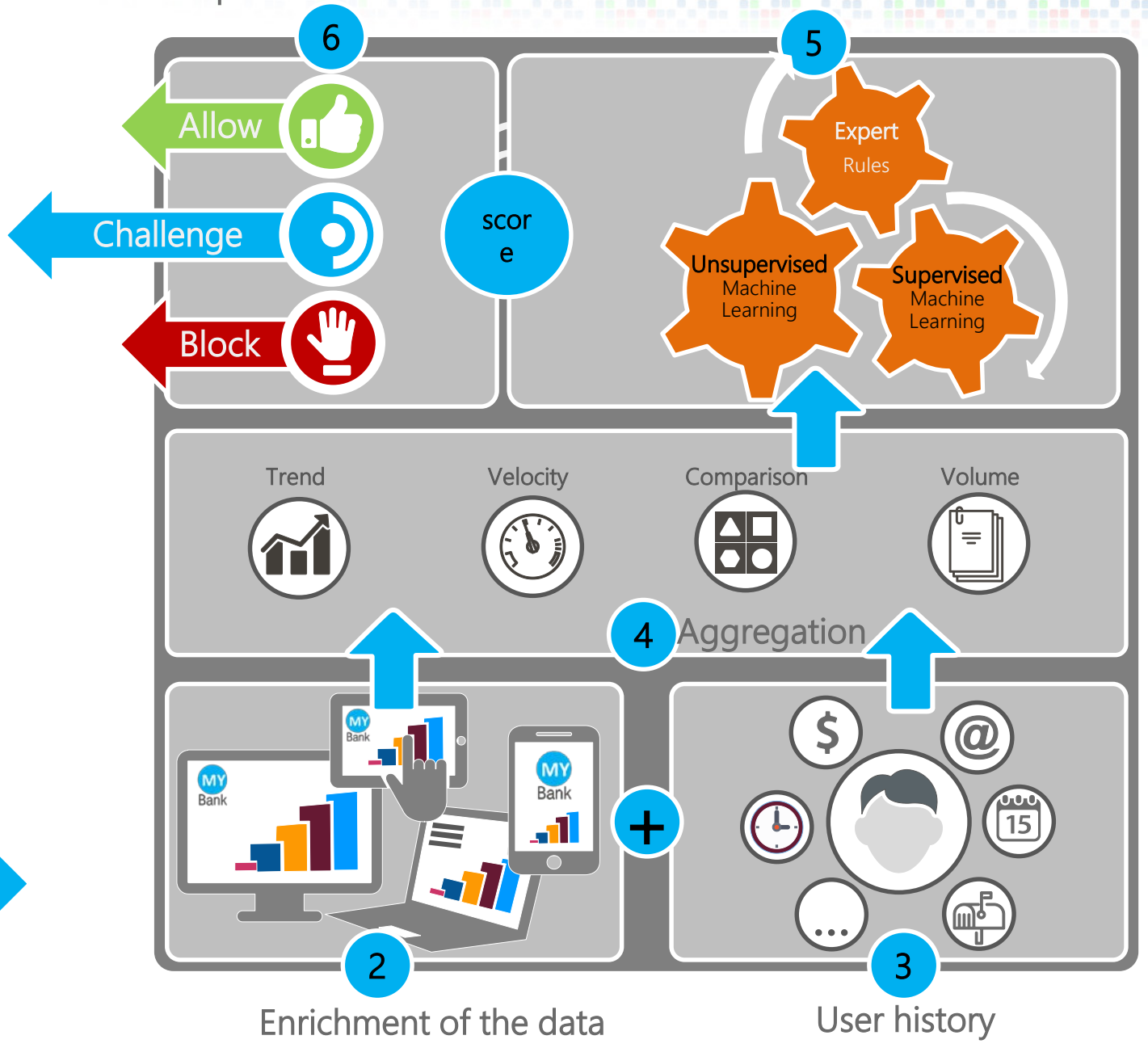
The diagram illustrates a security process. A hand holds a smartphone on the left showing a notification: '17:42 Tuesday 30 September MyBank You have a pending transaction for MyBank.' Another hand holds a smartphone on the right displaying transaction details: 'Foreign Transaction! Beneficiary Jim Robert IBAN F1548935472 Amount(\$) 250,00'. In the background, a tablet displays a banking app interface with 'Mybank.com' in the address bar and 'MY Bank' logo. A callout box with an eye icon points to the transaction details on the right phone, labeled 'Enhanced SWYS See What You Sign'. A line from the top text 'Device protected against cloning and compromise' points to the left phone. Another line from 'Notification is linked to encrypted transaction' points to the notification on the left phone. A third line from 'User is always aware' points to the transaction details on the right phone.

Fraud Prevention

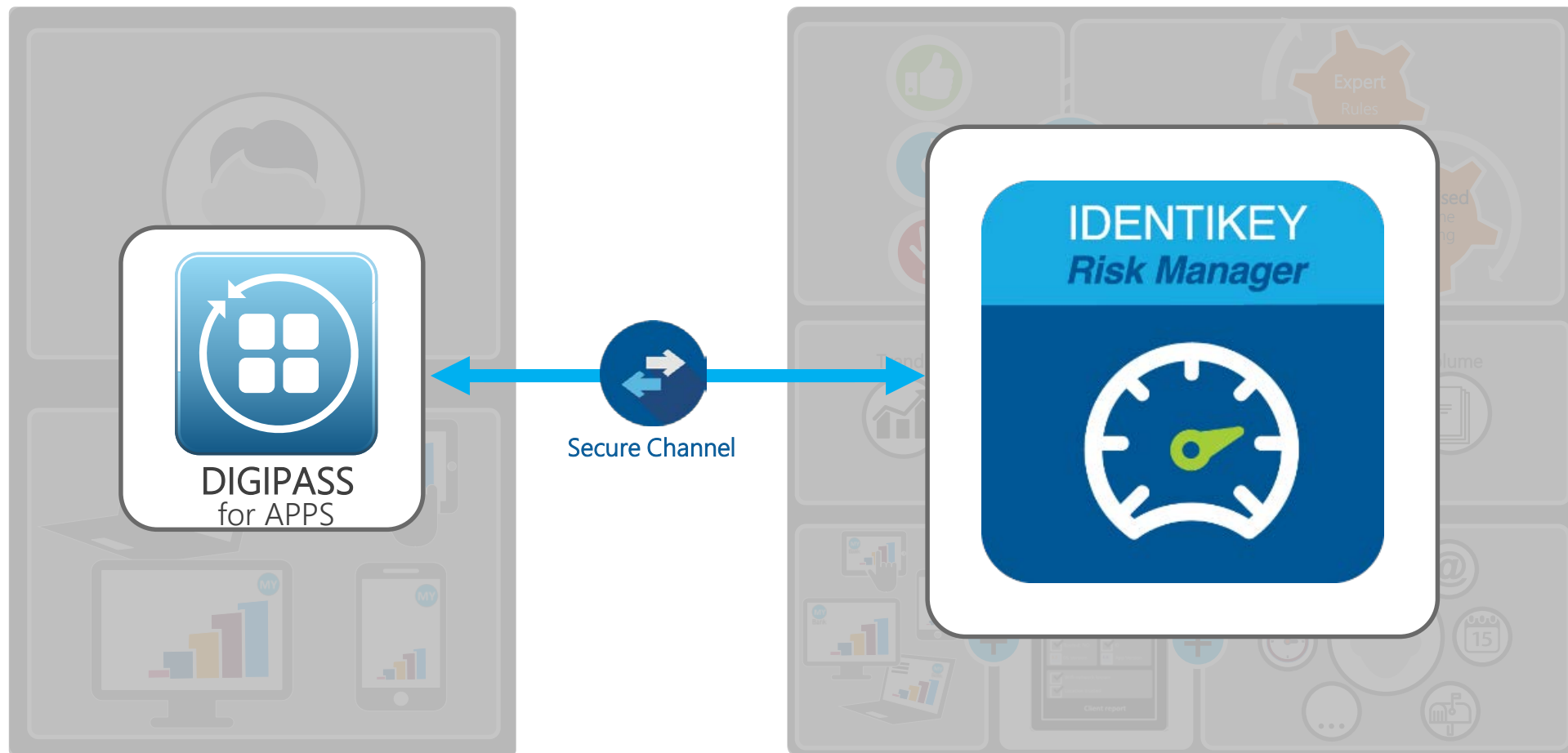


Response and Action

Analysis and Detection



VASCO's offering



Conclusion



Can banks provide a frictionless consumer experience via mobile wallets without sacrificing strong authentication and security in mobile payments?

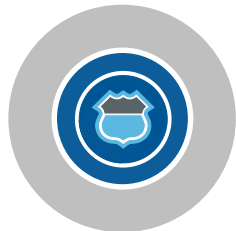
Multifactor Authentication Platform – using low friction or frictionless technology



Dynamic linking with secure channel technologies – Such as Vasco's Cronto code



Secure provisioning of personalized credentials



Mechanisms to prevent and detect alteration of mobile apps – via R.A.S.P. technologies



Yes by using the techniques described in this presentation it is possible to provide the frictionless experience whilst maintaining secure and complying with PSD2 regulations.

Fraud & Risk Manager – Such as Vasco's IRM

Forward Looking Statements

This presentation contains forward-looking statements within the meaning of Section 21E of the Securities Exchange Act of 1934, as amended, and Section 27A of the Securities Act of 1933, as amended. These forward-looking statements (1) are identified by use of terms and phrases such as "expect", "believe", "will", "anticipate", "emerging", "intend", "plan", "could", "may", "estimate", "should", "objective", "goal", "possible", "potential", "project" and similar words and expressions, but such words and phrases are not the exclusive means of identifying them, and (2) are subject to risks and uncertainties and represent our present expectations or beliefs concerning future events. VASCO cautions that the forward-looking statements are qualified by important factors that could cause actual results to differ materially from those in the forward-looking statements. These risks, uncertainties and other factors include the risk related to VASCO's ability to integrate acquisitions into the business of VASCO successfully and the amount of time and expense spent and incurred in connection with the integration; the risk that the revenue synergies, cost savings and other economic benefits that VASCO anticipates as a result of an acquisition are not fully realized or take longer to realize than expected; and the risks, uncertainties and other factors that have been described in our Annual Report on Form 10-K for the year ended December 31, 2015, and those discussed in other documents we file with the SEC, which include, but are not limited to, (a) risks of general market conditions, including currency fluctuations and the uncertainties resulting from turmoil in world economic and financial markets, (b) risks inherent to the information security industry, including rapidly changing technology, evolving industry standards, increasingly sophisticated hacking attempts, increasing numbers of patent infringement claims, changes in customer requirements, price competitive bidding, and changing government regulations, and (c) risks specific to VASCO, including, demand for our products and services, transition from hardware to software products, competition from more established firms and others, pressures on price levels and our historical dependence on relatively few products and regions, certain suppliers and certain key customers. Thus, the results that we actually achieve may differ materially from any anticipated results included in, or implied by these statements. Except for our ongoing obligations to disclose material information as required by the U.S. federal securities laws, we do not undertake any obligations or have any intention to release publicly any revisions or updates to any forward-looking statements to reflect events or circumstances in the future or to reflect the occurrence of unanticipated events or for any other reason.

Copyright & Trademarks

Copyright

Copyright © 2016 VASCO Data Security, Inc., VASCO Data Security International GmbH. All rights reserved.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior written permission of VASCO Data Security.

Trademarks

VASCO®, VACMAN®, IDENTIKEY®, DIGIPASS®, MYDIGIPASS™, CRONTO®, the (V) logo, and eSignLive™ are registered or unregistered trademarks of VASCO Data Security, Inc. and/or VASCO Data Security International GmbH, or Silanis Technology Inc. in the U.S. and other countries.

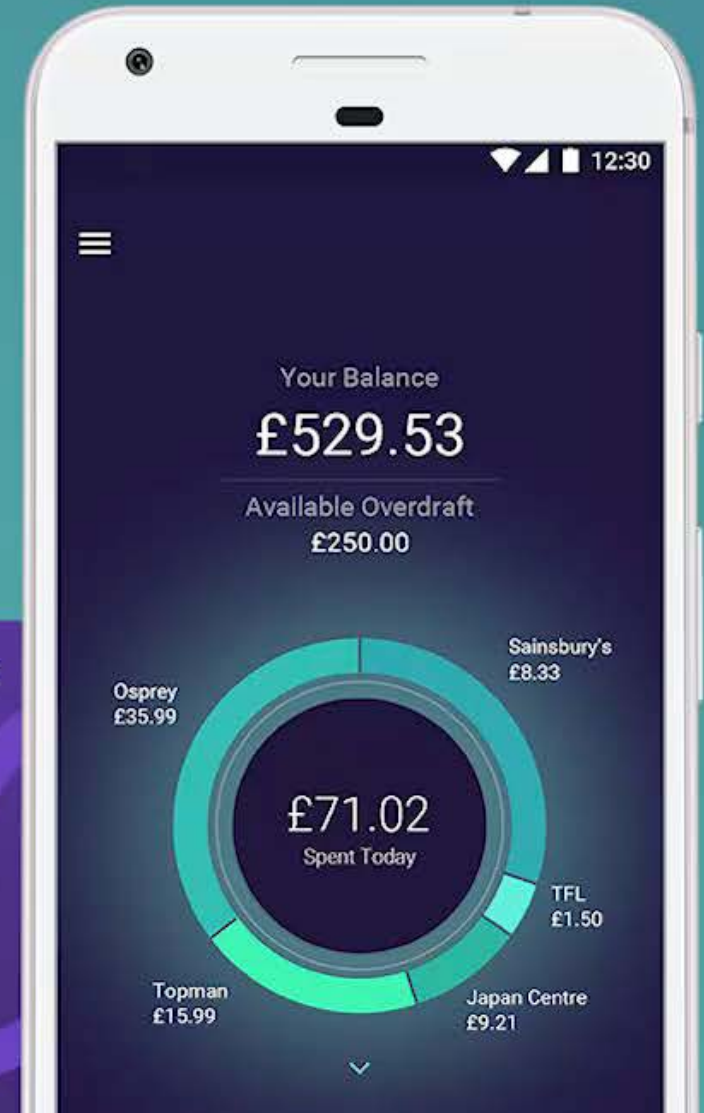
Starling Bank

Julian Sawyer

www.starlingbank.com @starlingbank

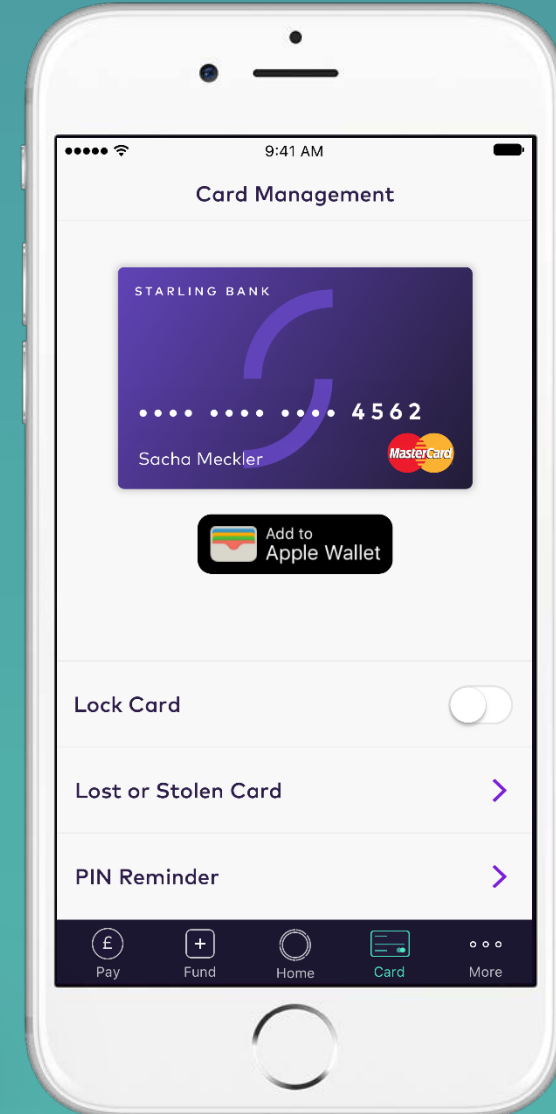
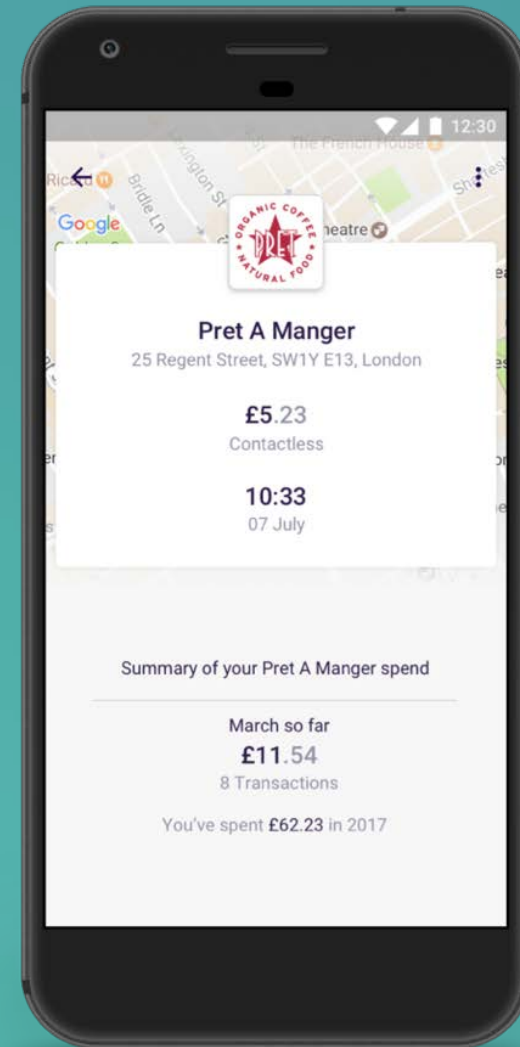
Starling Bank

- Tech start-up with a banking licence
- 100% cloud based, Mobile only
- MasterCard debit card
- Faster Payments & Direct Debits
- Spending Insights
- Card Control
- Developer platform & Marketplace



Creating an amazing customer experience in payments

- Choice
- Focus
- Speed



Starling Bank

Julian Sawyer

www.starlingbank.com @starlingbank

Thank you to speakers

- Dan McLoughlin, Regional Technical Account Manager, VASCO Data Security
- Julian Sawyer, COO, Starling Bank