EMV® 3-D Secure and Mastercard® Identity Check™

Smart payments demand smart security

October 2018

Presenters Name

mastercard.

Keeping payments secure in a connected world

Structural opportunities to address:

1. Accelerated shift to digital payments and increased card-not-present fraud

a) **Reduce friction** during authentication process

b) Reduce fraud and **false declines**

c) Reduce **declined transactions** & improve UX @ trusted merchants

2. New regulation

- **Strong Customer Authentication** (SCA) is new standard
- Smart management of SCA exemptions is essential

3. Enhanced consumer expectations

- «Make it **simple & secure** across all channels»
- «I want to stay in **control** of my spending»

©2017 MasterCard. Proprietary and Confidential

The challenges in the digital payments landscape are creating the need for better authentication

Digital commerce continues to grow—with a greater share via mobile. With this growth and the global migration to EMV chip in the physical world, card-not-present (CNP) continues to be the main area of card fraud. But consumers expect digital payments to be as simple and secure as in the physical world.

DIGITAL PAYMENTS HAVE LOWER APPROVAL RATES.

97% vs. 85% is the gap between physical and digital approval rates in Europe[1]

DIGITAL PAYMENTS HAVE HIGHER FRAUD RATES

>10x higher is the digital fraud vs. physical in Europe – together with lower approval rates this holds the risk of negative impact on usage and attrition[1]

THE MAJORITY OF FRAUD IS CNP

>75% of total card fraud in the region is from card-not-present (CNP) —and in most markets is on the rise[2]

1.MASTERCARD. JANUARY THROUGH NOVEMBER 2017 DATA, ACROSS ALL CARD TYPES. 2017.
2. EUROMONITOR, FICO. 2016.

©2018 MasterCard. |Proprietary|Confidential

Current authentication tools and methods don't meet the need for simple and secure payments

Consumers are impacted by **fraud and high false decline rates**

>1/3 Consumers are concerned about card fraud[2], still one out of five uses the same password for every website[7]

1 out of 3 Transactions declined due to suspected fraud are believed to be legitimate[4]

Merchants hesitate to adopt new technologies **and lose revenue**

62% Of breaches could have been prevented by stronger authentication methods such as dynamic passwords and biometrics[3]

20-25% online purchases in Europe are abandoned before completion[1]

Issuers are confronted by **growing competition and regulation issues**

1/3 Europeans say they use their replacement card less, post fraud—with more than 1 out of 10 actually switching banks[5]

up to 23% Of payment revenue is at risk for European issuers within the next five years, from digital disruptors[6]

1. DIGITAS LBI. DIGITAL. CONNECTED COMMERCE SURVEY. 2017 2 AITÉ. GLOBAL SECURITY ENGAGEMENT SCORECARD. 2016 3 VERIZON. DATA PASSWORDS BREACH INVESTIGATIONS REPORT. 2015 4 JAVELIN. FUTURE-PROOFING CARD AUTHORIZATION. 2015 5 AITE. GLOBAL CONSUMER CARD FRAUD: WHERE CARD FRAUD IS COMING FROM. 2016 6 . MCKINSEY. A BRAVE NEW WORLD FOR GLOBAL BANKING. 2016 7 ACCENTURE. DIGITAL CONSUMER SURVEY OF 24,000 CONSUMERS IN 24 COUNTRIES. 2015

©2017 MasterCard. Proprietary and Confidential

The new 3-D Secure standard allows to drive greater security and profitability – while enhancing the user experience (UX) for your cardholders

	3DS 1 Standards	NEW EMV 3DS Standards	Benefits of NEW EMV 3DS
METHOD	Static passwords/ security questions	Eliminates static pass-words for stronger two-factor authentication	• Greater security • Greater convenience
INTERFACES	Browser dependent	Supports new payment needs, such as in-app and mobile payments	• Better UX • Wider applications
DATA	Only 15 data elements available	Enables 10X more data to be exchanged	• Improved decisioning
USE CASES	Supports guest check-out only	Supports additional use cases , e.g. Card on File, wallets, tokenization, etc.	• Expanded use • Greater security
DECISIONING	Merchants bound by issuer decisioning	Enhances decisioning by increased merchant flow of data	• Greater flexibility

Mastercard Proprietary and Confidential

Mastercard Identity Check is leveraging the updated EMV 3-D Secure protocol to help you reduce fraud and false declines of card-not-present transactions – while providing cardholders with a friction-free checkout experience, so that you can take full advantage of the fast growing e-commerce business.

SOLUTION

Mastercard Identity Check helps improve digital payments security and increase approvals – while offering a frictionless payment experience to cardholders

- ✓ **Mastercard Identity Check** is a **next generation authentication solution** that enables **greater security** and a **user-friendly** digital payment experience.
- ✓ It helps **reduce fraud, false declines and unnecessary friction** - while meeting **Strong Customer Authentication** (SCA) requirements under the PSD2 regulation.
- ✓ Mastercard Identity Check **leverages the new EMV 3-D Secure protocol** with the power to exchange 10X more data between merchants and issuers, including new mobile capabilities – raising the bar on authentication.

mastercard ID Check

©2017 MasterCard. Proprietary and Confidential

Mastercard Identity Check builds upon the enhanced EMV 3DS protocol to address digital payment changes and challenges

Secure Code (based on 3DS1 Standards)	**Mastercard Identity Check** (based on NEW EMV 3DS Standards, replaces Secure Code)
MasterCard SecureCode	mastercard ID Check
Multiple authentication methods 	**Biometric**-based authentication Fingerprint Face Voice Eye with SMS OTP + 1 factor as back-up
▪ Web only ▪ Limited data ▪ Payments only	▪ **Multiple channels** (web and mobile App) ▪ Much **more data and options** (to better manage the risk) ▪ Payments **and beyond**

With Identity Check you can benefit from the following assets :

- Mastercard **Authentication Network**
- Updated **EMV 3DS** Protocol
- **Authentication Standards** Guide
- Standards for **Merchant White Listing**
- Core Functions **Specifications**
- Continuous **Innovation** (biometrics, RBA, behavioral analytics, AI…)
- **Tested solution**, designed to reduce resource needs and time to market
- **Plug-in-Play Biometrics** (mobile solution to help secure digital payments, mobile banking, and other channels)

©2017 Mastercard. Proprietary and Confidential

Migrating to EMV 3-D Secure and Mastercard Identity Check offers clear benefits

Eliminates static passwords for **Strong Consumer Authentication (SCA)** - based on the use of two or more elements - across all devices in real-time

Supports new payment needs, like authorization via mobile devices or in-app payments

Delivers a **better online payment experience for consumers…**

…by **reducing cardholder verification needs:** risk-based authentication (RBA) allows most transactions to be approved directly and without cardholder interaction, only challenging higher-risk transactions to be validated using SCA

…by offering simple and intuitive options for **consumers to verify their identity if needed**, supporting biometrics, dynamic passwords, security questions, plus proprietary options

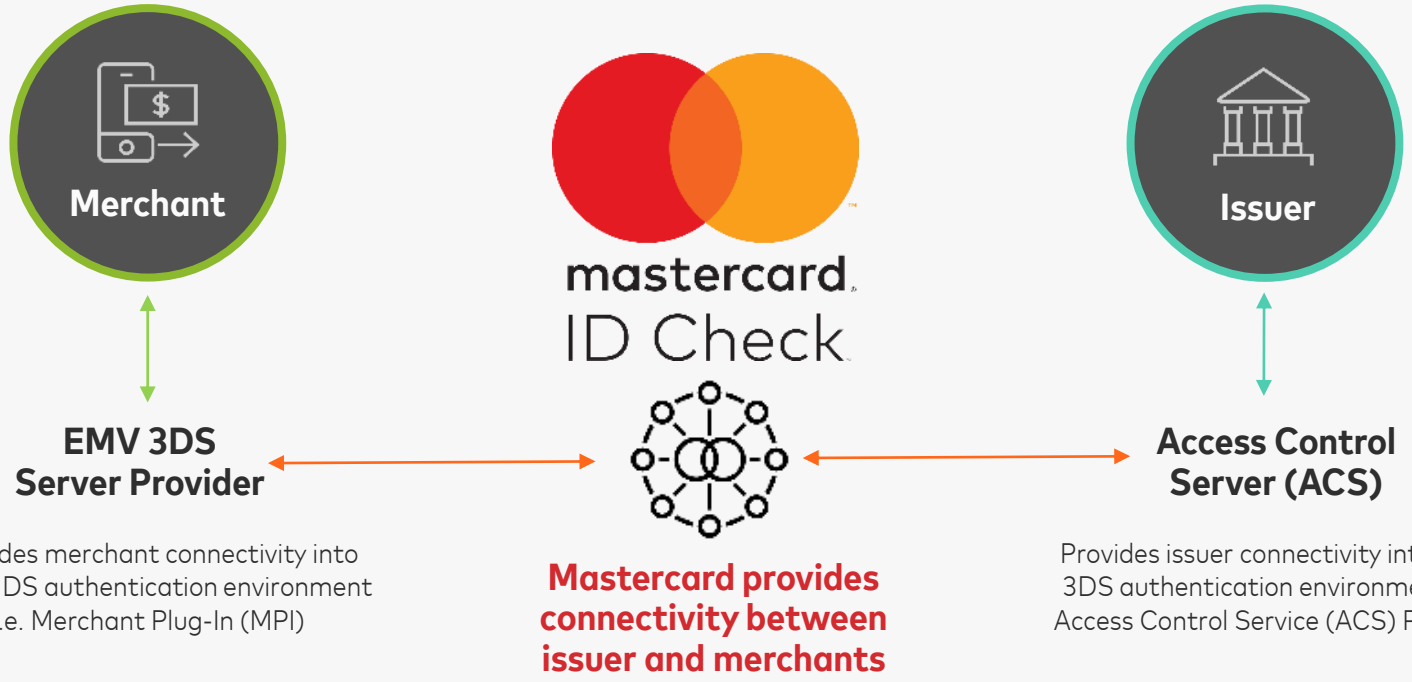
…by driving frictionless alternatives, like Credentials-On-File (COF) or Whitelisting, as a result of connecting issuers and merchants to drive data exchange

Can be **seamlessly integrated** into the merchant's checkout process

Offers the flexibility to address enhanced issuers needs, such as **securing banking applications, out-of-band authentication**, etc.

©2017 MasterCard. Proprietary and Confidential

Merchants and Issuers participate in EMV 3DS via third party service providers with Mastercard as the connecting link



©2017 MasterCard. Proprietary and Confidential

Identity Check seamlessly integrates into the transaction flow to deliver secure authentication

With Identity Check & EMV 3DS

CARDHOLDER

MERCHANT

MASTERCARD

ISSUER/ ACS PROVIDER

1. Begins the checkout process

2. **Initiates authentication request**—via their 3DS server provider

3. **Routes the request** to the appropriate issuer via the authentication network

4. **Receives and performs risk-based authentication** (i.e., scoring and rules)

5. If the risk is **below** defined thresholds the **response is to fully authenticate**

   If the risk is **above** defined thresholds the **response can be for further validation or decline authentication**

6. **Receives the response and decides** to submit for authorization

Consumers now can easily prove their identity, if needed with dynamic passwords or biometrics

Merchants have greater ability to share information with issuer to help improve risk models

Issuers/ACS providers now can receive 10X more data to help them make more informed decisions

©2017 MasterCard Proprietary and Confidential

Identity Check is simple and easy for cardholders to use

If the cardholder is required to authenticate themselves at checkout, the issuer can insert intelligent friction in multiple ways

EMV 3-D Secure Transaction Authentication

Frictionless Flow
Majority of transactions

Risk Based Authentication (RBA)

Risk Based Authentication utilizes the rich data exchange provided via EMV 3-D Secure to determine risk.

Transcactions deemed low risk may be silently authenticated without unnecessary friction—while higher risk transactions can be prompted for cardholder authentication resulting in:

- Vast majority of cardholder experiences are seamless with no friction
- "Silent" authentication happens in the background, without the consumer awareness of the process after they initiate payment

Intelligent Friction
Minority of transactions

Biometrics

- The cardholder is prompted to authenticate on mobile device
- Authenticates with pre-selected biometric method: fingerprint, face, voice, other.

One Time Password

(fallback solution)*

- Cardholder receives a one-time use code through the mobile banking app or via SMS text message from issuer
- Enters code on the authentication page and is verified as correct

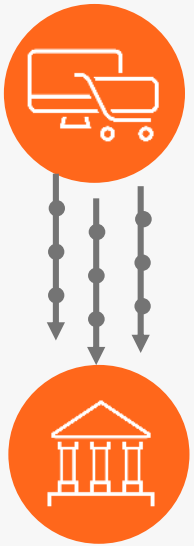
* THIS MAY REQUIRE AN ADDITIONAL KNOWLEDGE FACTORY TO COMPLY WITH THE EBA REGULATORY TECHNICAL STANDARDS (RTS)

EMV 3-D Secure comes with a list of new benefits for merchants, too

EMV 3DS addresses a number of key limitations of the previous 3-D Secure 1 protocol. It is projected to become one of the strongest solutions in the fight against card-not-present (CNP) fraud - without sacrificing the shopping experience

Key changes include:

- **More robust security** to fight fraudulent online transactions – through strong customer authentication, such as biometric and token-based authentication, instead of static passwords
- **Compatibility with mobile devices**, to reflect the growing m-Commerce trend, including in-app payments
- **Improved Risk Based Authentication (RBA)** through the exchange of significantly more contextual data related to the purchase than possible with 3DS 1
- **A frictionless user experience** to reduce shopping cart abandonment



With EMV 3DS merchants can share more contextual data with issuers – which creates a win-win-win situation

- ✓ Having more data to analyze with each transaction enables issuers to apply a **more accurate risk assessment** and approve most transactions based on risk based authentication (RBA).
- ✓ Getting most transactions approved based on RBA empowers merchants to offer a **frictionless checkout experience** for the cardholder without compromising on strong security
- ✓ Enjoying a frictionless checkout experience reduces cart abandonment and increases **consumer satisfaction and loyalty**

©2017 MasterCard Proprietary and Confidential

Applied strategically, authentication can help drive results

Increase Approvals

+10pp

Increase in approvals when transactions are fully authenticated[1]

Stronger authentication can help balance an optimized user experience with reduced fraud

Reduce Fraud

-50%

lower digital fraud when dynamic authentication is used[1]

©2017 MasterCard. Proprietary and Confidential

1. MASTERCARD 2017 DATA - Contact your Mastercard representative to engage in a quantification effort specific to your business.

Mastercard can help you start the transition process in three simple steps

	Financial Institutions	Merchants
1 SELECT	Access Control Service (ACS) Provider	EMV 3DS Merchant Integrator
2 REVIEW	Mastercard Identity Check branding requirements	Mastercard Identity Check branding requirements and implementation guide
3 REGISTER	In Onboarding process (includes adopting updated authentication challenge flows)	In Onboarding process
ADDITIONAL SUPPORT/ OPTIONS	Consider RBA for frictionless authentication on low risk transactions.	API connection for select merchants and MPGS solution (October 2018)

Risk Based Authentication (RBA) can help optimize the consumer experience—via industry leading analysis to drive frictionless authentication, including situations where the issuer/ACS provider is not able to respond*

Please see the Mastercard Identity Check Guide on Mastercard Connect® for detailed standards

*WHERE PERMISSIBLE BY REGULATION

©2018 Mastercard. Proprietary and Confidential.

KEY TAKE AWAY

In summary: Mastercard Identity check meets the need for simple and secure payments and helps everyone 'win' from EMV 3DS and PSD2

Consumers

- **Eliminates the frustration** of managing and remembering passwords
- Provides strong **protection** for financial data
- **Minimizes disruptions** due to decrease in fraud by 50% (fully authenticated vs. 'merchant only' transactions[3])

Merchants

- **Helps drive revenue** by reducing cart abandonment of up to 70% when biometric identification is used[1]
- Hassle-free authentication can help merchants **gain greater share** in their category
- Authenticated transactions have **higher approval rates of** +10pp[2]

Financial Institutions

- **Decreases fraud** by eliminating the risk from passwords
- Enhances cardholder **engagement** and loyalty[4]
- Increases revenues via **increased completed transactions**
- **Lower customer service costs** due to fewer calls and password resets

1. IDENTITY CHECK PROGRAM AND EMV 3-D SECURE VERSION 2 (EMV 3DS) UPDATE. 2017.
2. MASTERCARD. JANUARY THROUGH NOVEMBER 2017 DATA, ACROSS ALL CARD TYPES. 2017. 3. MASTERCARD DAT, 2017 .
4 AMERICAN GRAPHICS INSTITUTE. ROI OF UX: HOW USER EXPERIENCE IMPACTS BUSINESS SUCCESS. 2017

©2017 MasterCard. Proprietary and Confidential

Key recommendations

1

Design the best SCA user-experience (UX)

One SCA UX for all purposes including in e-commerce, e-banking, call center

2

Deploy the best SCA solutions

- Biometrics
- One-time password SMS as fallback*
- Push notifications

3

Enable and maximize the frictionless flow

- Develop Whitelisting
- Enable TRA exemption by using RBA and respecting fraud ratio thresholds

4

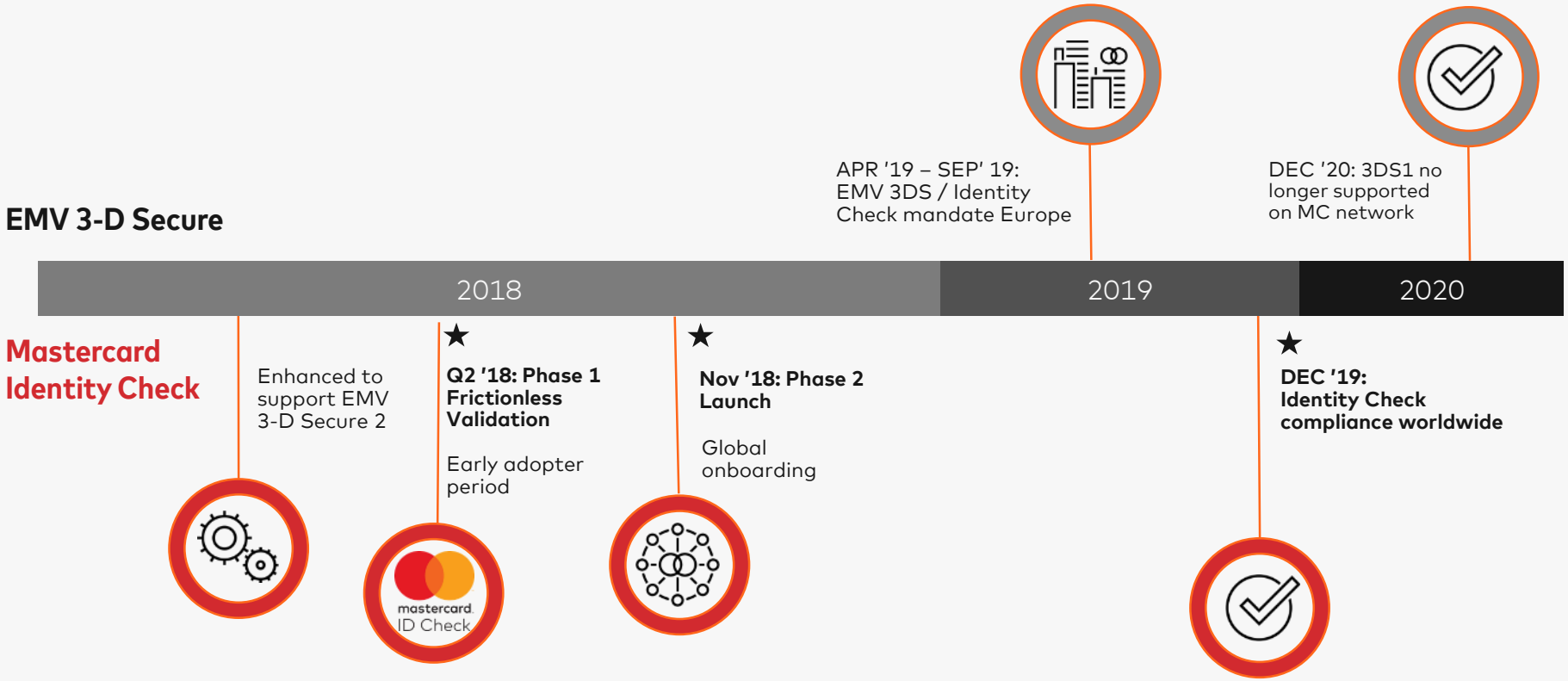
Educate your customer base

Stakeholder education (cardholders, branch-tellers, merchants) about the new authentication experience and its advantage will be a key enabler

©2017 MasterCard Proprietary and Confidential

- THIS MAY REQUIRE AN ADDITIONAL KNOWLEDGE FACTORY TO COMPLY WITH THE EBA REGULATORY TECHNICAL STANDARDS (RTS)

Timeline: Migrating from SecureCode / 3-D Secure 1 to Identity Check / new EMV 3-D Secure



©2017 MasterCard. Proprietary and Confidential

Let's get started

- **Review** how EMV 3-D Secure can help ensure a positive user experience
- **Discuss** current card-not-present authentication solutions to see how Mastercard can help increase approvals
- **Demo** Mastercard Identity Check
- **Map-out** how Identity Check can be part of your authentication strategy

©2017 Mastercard. Proprietary and Confidential.

Take the right approach and apply a holistic view to digital security - with **Mastercard's Digital Security Roadmap**:
A comprehensive plan with actionable solutions to help you tap into the opportunities of the digital payments world

Digital Payments are becoming the **new standard**

- and financial services providers need to keep up to stay relevant

Unfriendly Authentication

20 to 25% of online purchases in Europe are abandoned before completion[1]

Fraud & False Declines

75% of card fraud in Europe is CNP fraud — and most markets on the rise[2]

Lower Approval Rates

Approval rates digital payments: 86% (vs. 97% in card present payments) [3]

Payment Services Directive (PSD2):

Decreasing online fraud by increasing the number of transactions subject to

Strong Customer Authentication (SCA)

mastercard.

DIGITAL SECURITY ROADMAP

REDUCE FRICTION

- Mastercard **Identity Check** and EMV **3D-Secure**
- **Biometric** authentication (min. 1 method), e.g. Mastercard **ID Check Mobile**

REDUCE FRAUD & FALSE DECLINES

- Mastercard **Decision Intelligence** – when fraud is >13bps
- Mobile **Transaction Alerts**, like **Mastercard Spend Alerts**

REDUCE LOST TXNS

- Mastercard **Automatic Billing Updater** (ABU)
- **Merchant whitelisting** for trusted beneficiaries

- ✓ Maintain direct **relationship** with your cardholders
- ✓ Positively influence your P&L by reducing costs and increasing **revenues**
- ✓ Compliance with PSD2 **regulation**

1 MASTERCARD ---- 2 SOURCE: JAVELIN ADVISORY SERVICES, FUTURE PROOFING CARD AUTHORIZATION ---- 3 MASTERCARD. Q1 - Q3 2016 DATA, ACROSS ALL CARD TYPES. 2016

Mastercard Identity Check offers a mobile biometric solution to secure digital payments and mobile banking applications

App-based hosted solution leveraging the mobile device to secure online payments and mobile banking applications

Comprised of two main components

1. Front-end biometric **app** that supports both fingerprint and facial recognition
2. Back-end biometric **authentication platform**

Plug and Play Deployment models through our SDK

Software Development Kit (SDK) for Issuer's Mobile Apps

Integrated into issuer app; used for mobile banking, call center, suspicious transactions and digital payments

Biometric authenticators available

- ✓ Fingerprint (Touch ID, Android Finger)
- ✓ Facial recognition
- ✓ Face ID
- ✓ Voice recognition

H2
- ○ Samsung Iris

H2
- ○ Passive Biometrics (NuData)

©2017 MasterCard. Proprietary and Confidential