New Approaches for Customer Authentication Across Channels

Janet Smith
Senior Vice President, Identity Solutions
Mastercard Worldwide

Authentication is critical to the payment industry

Payments in the digital world should be as safe and simple as they are in the physical world

The challenge…

	Approval Rate[1]	Fraud Rate[2]
Physical	96%	1x
Digital	83%	3x

Authentication can help…

Approval Rate[1] 11%	Transaction approval rates rise by 11% when fully authenticated
Fraud Rate[3] Less than 8 BPS	Issuers that implement dynamic authentication experience the lowest CNP fraud

1. Approval Rate Source: Mastercard Data Warehouse.
2. Fraud Rate Source: Javelin Strategy & Research, July 2013
3. Mastercard SecureCode cardholder verification method (CVM) fraud study, 2013.

MasterCard

Passwords still dominant…but in today's digitally connected world, they're are out-of-date with consumers' needs

- **Consumers use 5 digital devices on average**[1]
- **Time spent on mobile devices now surpasses desktops and laptops**[2]
- **Consumers have up to 30 online accounts requiring passwords**[3]

1 out of 5 consumers use the same password for every website[4]

60% of consumers find passwords "cumbersome"[7]

47% of consumers are using passwords over 5 years old[5]

84% of consumers admit forgetting their password[4]

>90% of user-generated passwords are vulnerable to hacking[6]

1. In 17 countries. Digitas, Connected Commerce Survey 2015.
2. eMarketer. Time Spent per Day with Major Media by US Adults, 2011–2017, 2015.
3. Identity Theft Resource Center. Consumers Fall Short on Using Strong Passwords. 2015.
4. Ketchum Global Research & Analytics, survey of consumers in 17 countries commissioned by Mastercard, 2015.
5. CBS Small Business Pulse. What's In A Password. Infographic. 2016.
6. Yahoo Finance. Your Password Isn't Safe. 2013.
7. Accenture Digital Consumer Survey of 24,000 consumers in 24 countries. 2015.

MasterCard

Consumers want an alternative to passwords —as do banks, merchants, regulators & everyone else…

Passwords are inconvenient and frustrating

Consumers resent the hoops they must jump through to prove who they are, and one-time passwords via SMS only increase checkout time and frustration. Security is important, but so is convenience.

Passwords are no match for today's fraudsters

And the problem will only get worse as EMV drives fraudsters to the online channel, increasing the risk of card-not-present (CNP) fraud.

Passwords will not meet new regulations

Regulatory bodies around the globe are beginning to mandate strong two-factor authentication.

Forgotten passwords cause abandoned shopping carts

About a third of online purchases are abandoned by cardholders at checkout because they can't remember their password.[1]

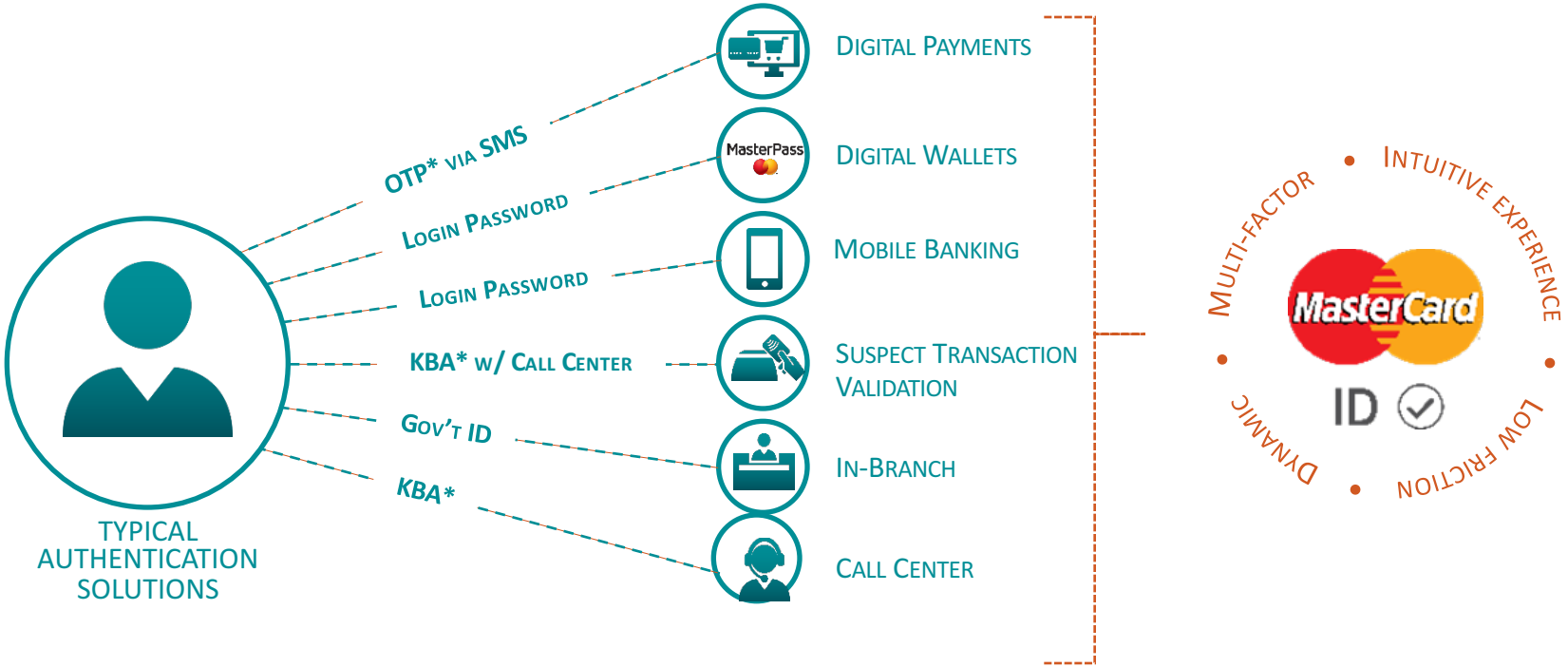
MasterCard

Consumers want service providers to recognize them in a single & consistent way across channels & devices…

Shaped by digital technology… today's consumer has high expectations for *convenience & security* in their financial transactions

MasterCard

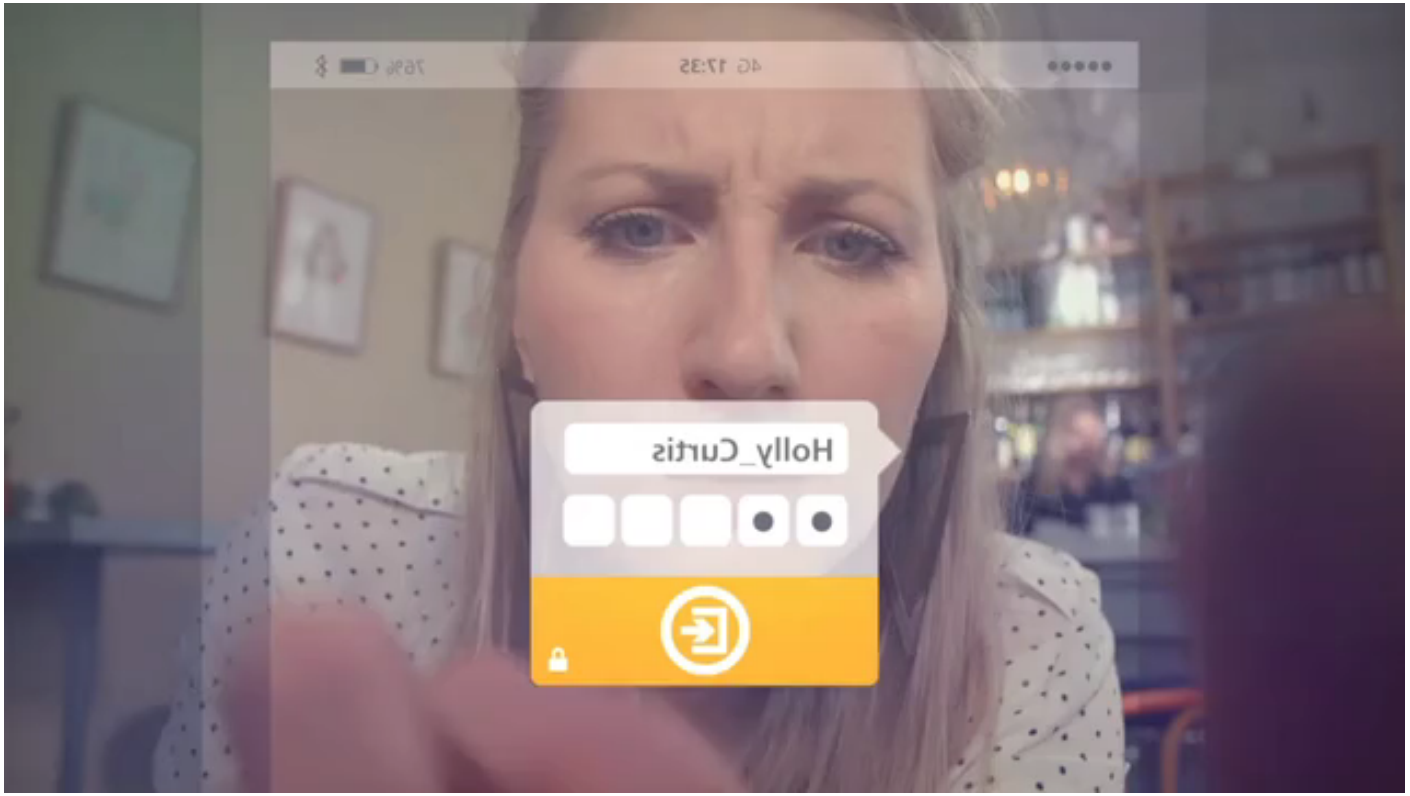
Mobile biometric authentication enables a single digital consumer identity across channels



*KBA: Knowledge Based Answer; OTP: One-time password

MasterCard

Transforming the Consumer Authentication Experience



Selfie Authentication https://www.youtube.com/watch?v=DfLarAas-U0
Fingerprint Authentication https://www.youtube.com/watch?v=m4qi3t1HP3g

MasterCard

Both consumers and financial institutions benefit from mobile biometric authentication

Consumer Benefits

- Provides a more **consistent**, satisfying experience at each authentication touchpoint
- **Eliminates the frustration** of managing and remembering passwords
- Provides **strong protection** for consumer's financial data
- Empempowers cardholders to control their **digital identity**

Financial Institution Benefits

- Delights **digitally savvy consumers** with an intuitive and consistent shopping and banking experience
- Addresses emerging **regulatory requirements** in many markets for strong two-factor authentication
- **Decreases** fraud and operational costs
- Enhances **customer engagement** and loyalty
- **Increases revenues** by enabling increased transaction completion and approval rates

MasterCard

Key Considerations When Implementing a Mobile Biometric Solution

TECHNICAL
LEGAL & REGULATORY

- **Not all device fingerprint sensors are created equal**…
  - Research & test the biometric false match & false accept rates before enabling a device for your solution
  - Ensure the biometric template storage on device is secure
- **New devices and OS upgrades** create opportunities & challenges, be prepared to constantly test and push out updates
- **Regulation & data privacy related to biometric usage varies by country** (sometimes it varies even within a country) and is ever-changing…invest in good legal counsel!

MasterCard

Key Considerations When Implementing a Mobile Biometric Solution

STRONG SECURITY & CONTROL

- **Take a layered approach to security**… utilize tools like device cryptography, device identification + biometrics to enhance security
- If you're bringing biometric data back to a central server for matching - **end-to-end communication channel encryption** is critical
- Make sure you understand and can **set the pass/fail thresholds** for biometric matching
- Don't store biometric data in a central server **– edge-based biometric matching** on the consumer's mobile device is best!

Key Considerations When Implementing a Mobile Biometric Solution

CONSUMER CONVENIENCE & CHOICE

- **Consumers want a choice of biometric modalities**, such as fingerprint, facial biometric, eye (vein or iris), voice…
- Some **biometric modalities are suited to certain authentication use cases** but not for others…voice is a great example of this!
- **Consumer usability testing is critical when** introducing a new biometric modality or mobile biometric use case.
- Ensure consumers can **enable multiple devices** with one enrollment

Questions?

janet.smith@mastercard.com

MasterCard