Securing card payments with standards

W3C Web Payments – TPAC 2018

October 22, 2018
Jonathan Grossar

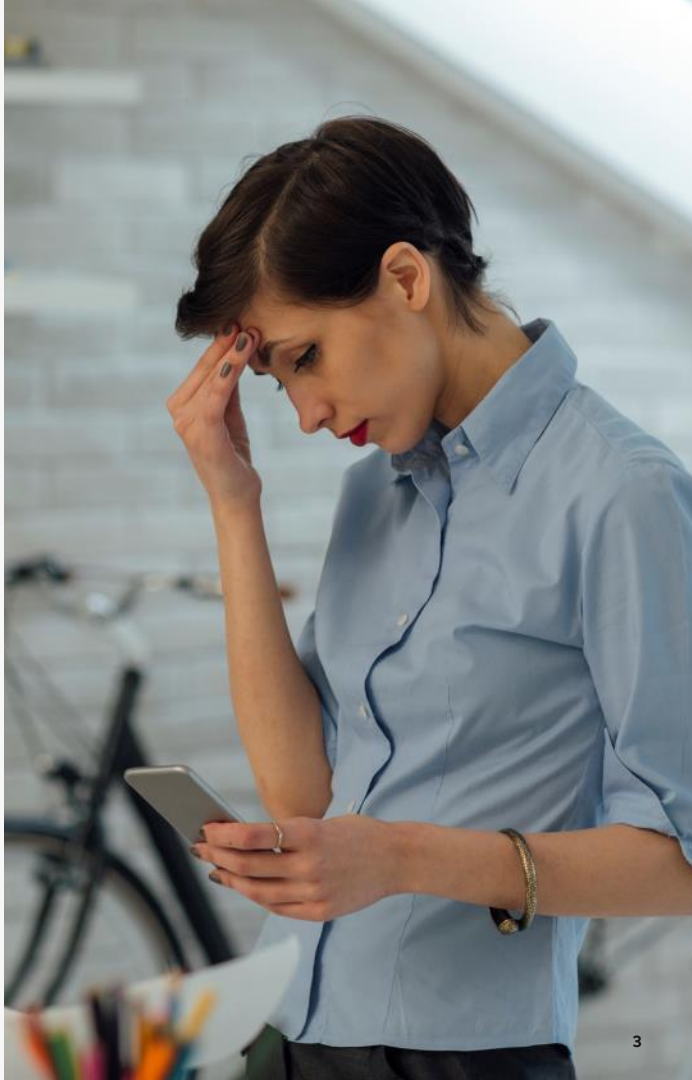
mastercard

We have a unique opportunity in W3C to make things right and turn web payments not only into a great user experience but also into a secure experience

mastercard

A secure experience is key – as digital friction, fraud, false declines, and poor authentication solutions are eroding consumer experience and merchant profitability

FRAUD	Up to $19.3B CNP Fraud is forecasted to rise from $11.5 billion in 2017 to $19.3 billion in 2022[1]	4X The amount of card not present fraud compared to card present rates[2]
APPROVAL	96% Physical Approval rate[2]	83% Digital Approval rate[2]
ABANDONMENT	$2.48 Cost of every $1 of fraud to organizations - meaning fraud costs them more than twice of the actual loss itself[3]	1/3 of false declined cardholders reduced or stopped shopping at the e-commerce merchants[4]



1. JUNIPER RESEARCH. ONLINE PAYMENT FRAUD: EMERGING THREATS, KEY VERTICAL STRATEGIES & MARKET FORECASTS
2. MASTERCARD. JANUARY THROUGH NOVEMBER 2017 DATA, ACROSS ALL CARD TYPES. 2017.
3. TRUE COST OF FRAUD STUDY. LEXIS-NEXIS
4. JAVELIN. OVERCOMING FALSE POSITIVES

Success in web payments will be determined by meeting stakeholders' expectations

Consumer, Issuer & Merchant Expectations

	Expectations
Consumer experience	• Frictionless and easy checkout • Better lifecycle management • Choice of privacy options • Consumer trust in payment, resulting in higher conversion rates
Increased security	• Reduce fraud • Reduce account data compromise and PCI exposure • Protection against Fraud and Account Takeover
Higher approval rates	• Decrease on False Declines • Improve approvals on cross-border transactions
Compliance with regulations	• Comply with local regulations (2-factor authentication, privacy etc.)

To secure the ecosystem, we need tokenization, consumer authentication, and more

Higher approval rates with increased security through

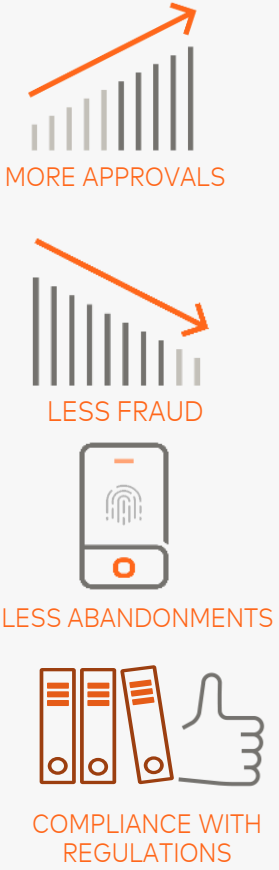
- Network tokenization
- Merchant registration

Higher conversion rates with consumer trust in payments through brand visuals (consumer knows what to expect)

Network tokenization + Merchant registration | **Consumer authentication** | **Consumer trust**

Less fraud with 3DS2 and risk-based authentication

Less abandonment with fewer step ups and user-friendly authentication with device authentication



mastercard

Network tokenization and merchant registration

We need to stop the propagation of plastic card numbers i.e. their distribution everywhere and to any entity requesting them

And replace them with

NETWORK TOKENS

- ❑ **Reduces impacts of account data compromise** or PCI exposure – through use of tokens with dynamic data (for consumer initiated transactions), and domain controls
- ❑ Improves **lifecycle management** – automatic token updates in case of card change, and no need for consumer to change card in case of account data compromise

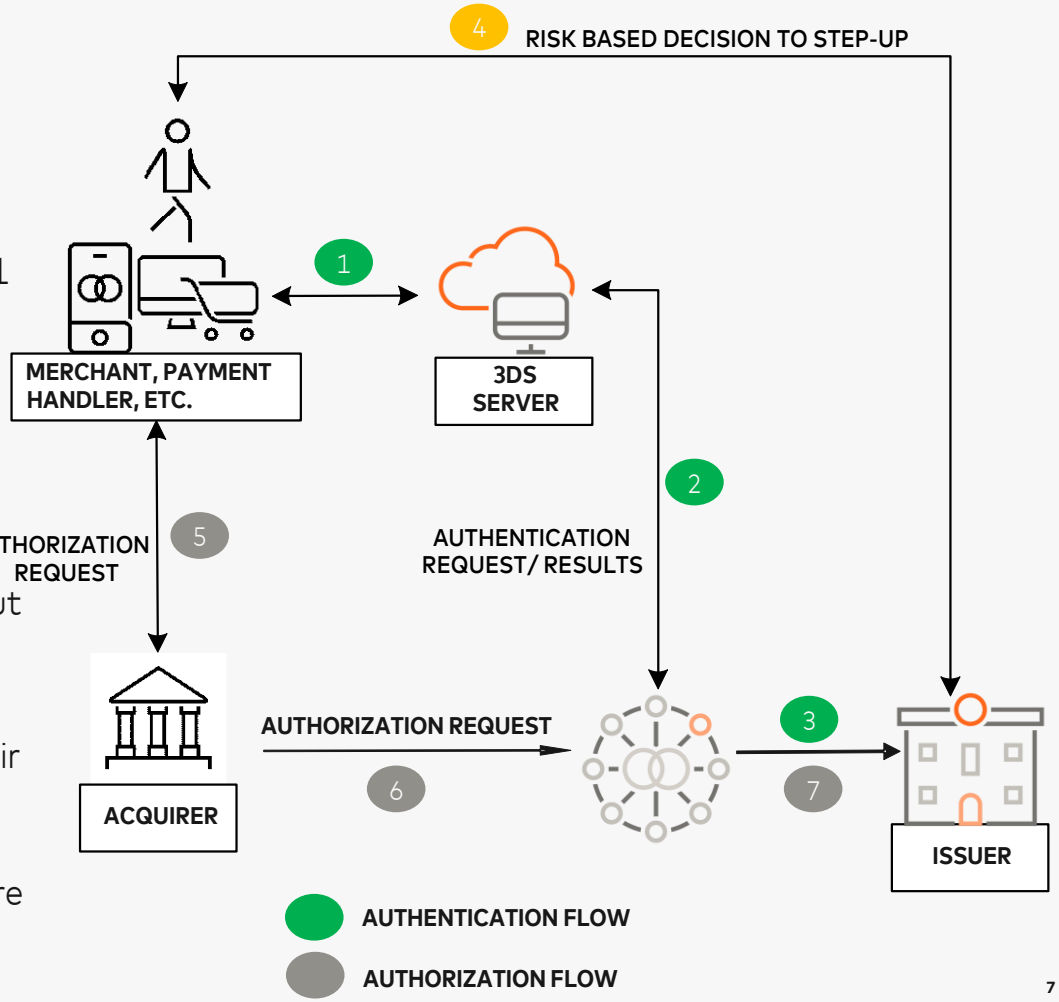
MERCHANT REGISTRATION

- ❑ Provides visibility on where the token is going to be used

Consumer authentication

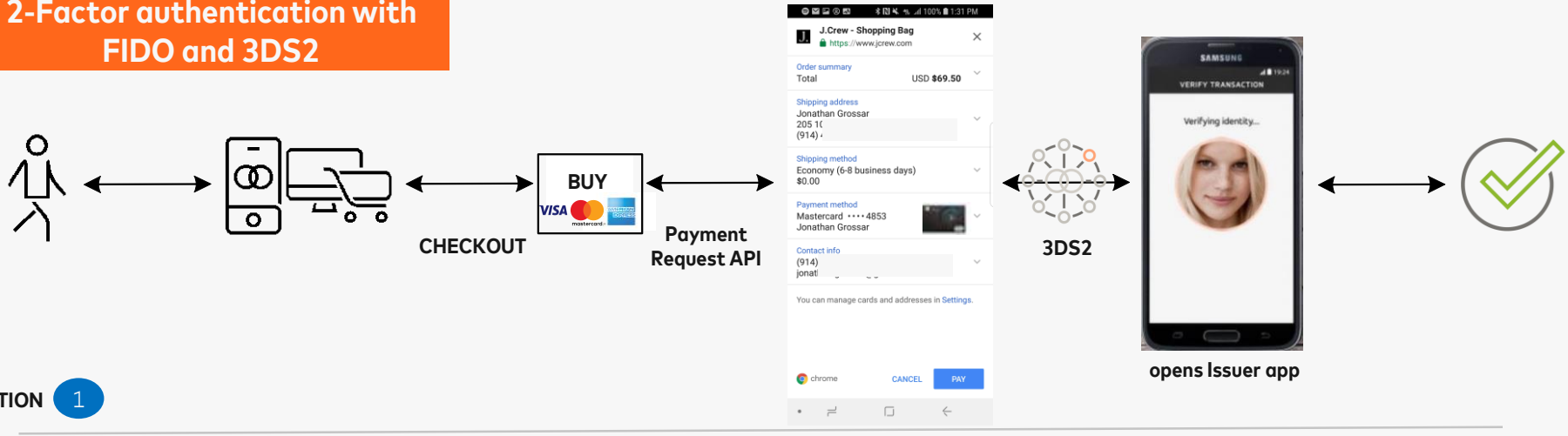
3DS2 benefits

1. **Risk-based authentication**
   - 3DS2 allows for 10X more data than 3DS1 to be exchanged
   - If authentication is not required per regulation, Issuers receiving 3DS2 data or risk signals should approve in most cases without step up (flows 1-2-3)
2. **Merchant choice**
   - Merchants may decide to use 3DS2 without authentication (flows 1-2 only)
3. **FIDO authentication (standardized in 3DS2)**
   - Performed by Issuer during step up (on their app), **or**
   - Performed by merchant/wallet prior to invoking 3DS2 i.e. authentication results are used as input to 3DS2 to remove need for Issuer step up



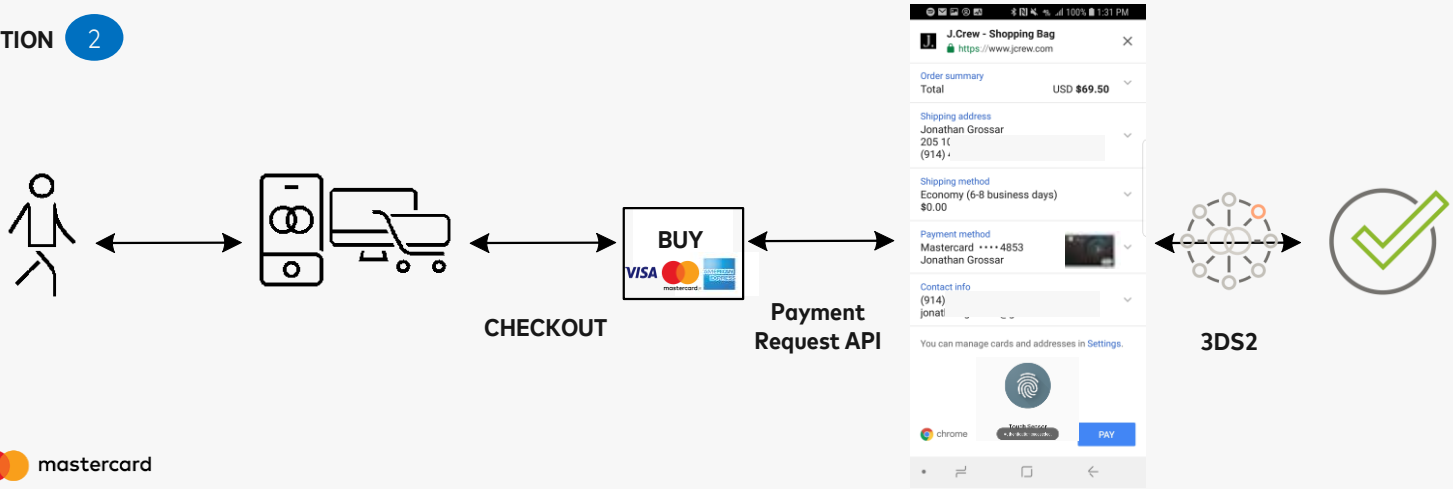
mastercard

2-Factor authentication with FIDO and 3DS2



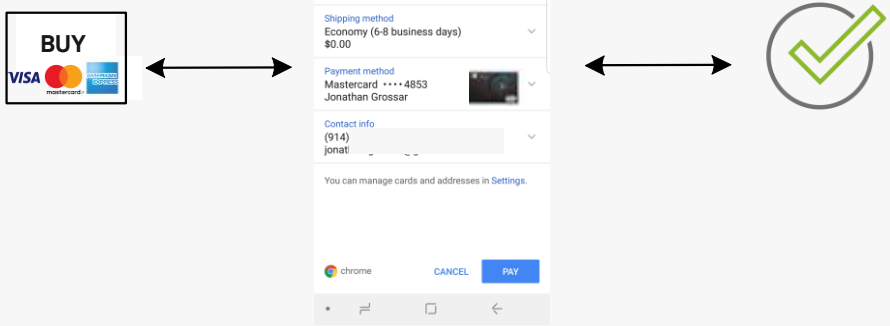
OPTION 1

OPTION 2



Consumer trust

We want to reassure consumers and provide them with full transparency on payment instruments when they pay



Know what to expect at checkout

Know what they can use at card selection

Know how they paid at transaction confirmation

We want to reassure consumers and provide them with privacy choices

Compliance with GDPR

mastercard

Let's not miss this fantastic opportunity to make it right!

What should be the next steps?

- Agree on the benefits to upgrade the infrastructure to use network tokens and consumer authentication
- Review EMV SRC specs and provide comments
  - Identify commonality with work done so far
  - Identify differences e.g. definition of roles, data collection
- Merge the tokenization and 3DS Task Forces into a single Task Force
- Include user-friendly FIDO authentication as part of 3DS2
- Review how to provide consumers with full transparency on payment instruments and with privacy options