EMV® 3-D Secure Data Elements

February 12, 2019

U.S. Payments Forum Mission

- *… the cross-industry body focused on supporting the **introduction and implementation of EMV and other new and emerging technologies** that protect the security of, and enhance opportunities for payment transactions within the U.S.*

Current EMV-related Topics and Issues

- Petro, Transit and Hospitality merchants EMV-enablement issues
- EMV contactless/mobile acceptance testing & certification
- Issuer considerations for contactless EMV (dual interface, offline data authentication)

Beyond EMV – Advanced Payments Topics and Issues

- Mobile payment and tokenization
- Authentication: biometrics, future of CVM, new signature requirements
- EMV 3-D Secure 2.0, Secure Remote Commerce and other CNP fraud tools

US PAYMENTS FORUM

Forum Activities & Resources

- **Collaboration on projects to develop resources to assist with U.S. EMV migration and implementation of other new and emerging payments technologies**
  - White papers, educational resources
  - Best practices and technical recommendations
- **Education programs for members and the industry**
  - Webinars, workshops, Forum member meeting tutorials, published resources
- **Communications**
  - Market outreach with recommended best practices and industry positions
- **Networking**
  - Forum for industry stakeholders to interact with all payments industry stakeholders

Information and resources available at www.uspaymentsforum.org

US PAYMENTS FORUM

Today's Speakers

- Randy Vanderhoof, U.S. Payments Forum

- Kristy Cook, Target, U.S. Payments Forum Steering Committee Chair

- Michael Horne, American Express

- Ian Poole, CardinalCommerce

US PAYMENTS FORUM

US Payments Forum: EMV 3DS Data Project

Goals

- Foster open discussion amongst merchants and issuers of new data elements in EMV 3DS
- Identify and share best practices to reduce gross fraud

*Guest attendance available for **merchants** and **issuers** interested in the discussion*
(email cmedich@uspaymentsforum.org)

Feb 12 Educational Webinar

Merchant & Issuer Prep Sessions

Merchant Focus: EMV 3DS data elements that have historically have indicated risk

Issuer Focus: generate questions for in-person discussion about the data elements and EMV 3DS

Mar11 In-Person Meeting
Phoenix, USPF

EMV® 3-D Secure Overview

Michael Horne, Sr. Product Manager, American Express

EMV 3-D Secure Overview

Remote commerce or e-commerce continues to grow worldwide. Payment transactions are occurring on various devices (e.g. mobile phones, tablets, PCs) where a high degree of e-commerce fraud can exist.

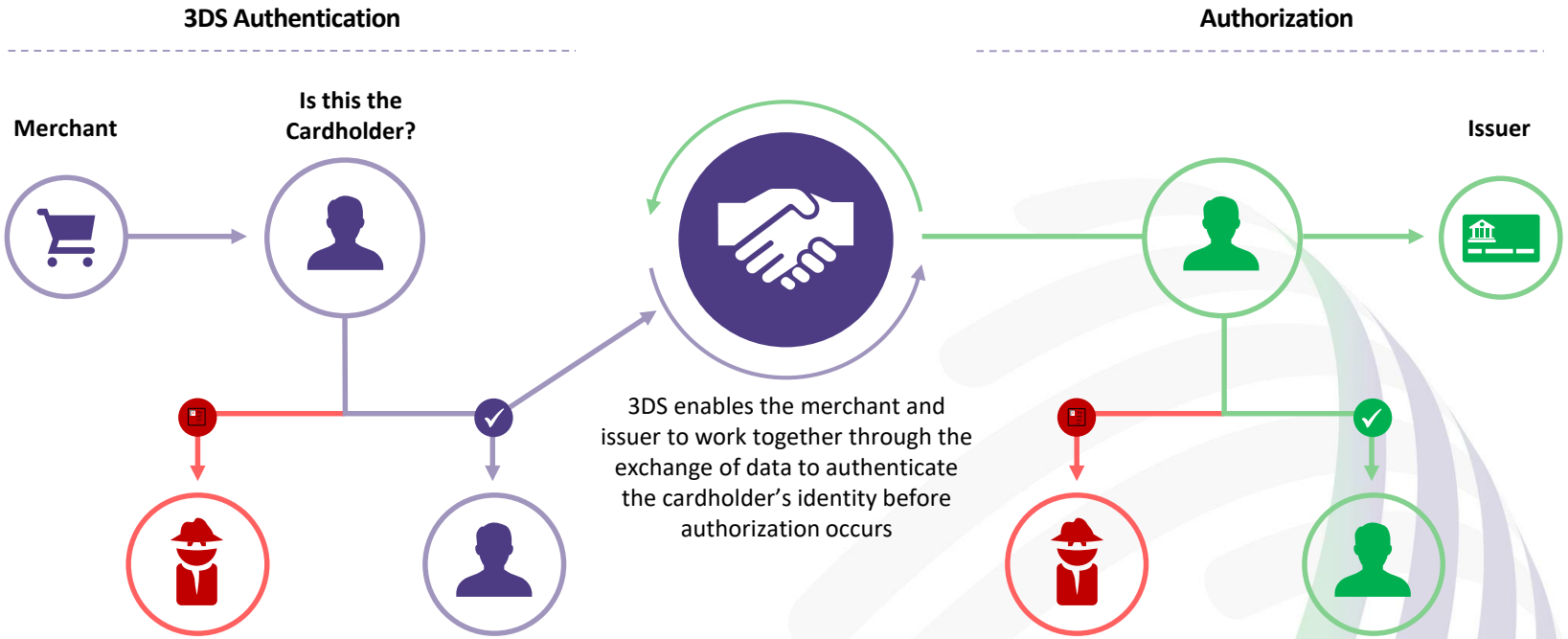
EMV® 3-D Secure (3DS)

Promotes an improved consumer experience when making e-commerce purchases by enabling intelligent risk-based decisioning.

- Allows for a rich data set to be exchanged between cardholder, merchant, and issuer
- Provides a secure communication channel between the cardholder, merchant, and issuer
- Enables issuers to authenticate their cardholder before transaction authorization

US PAYMENTS FORUM

How It Works


3DS Authentication
Authorization
Merchant
Is this the Cardholder?
Issuer
3DS enables the merchant and issuer to work together through the exchange of data to authenticate the cardholder's identity before authorization occurs
The cardholder's identity is verified by the issuer before the transaction is authorized
The 3DS authentication improves the issuer's confidence to authorize the transaction

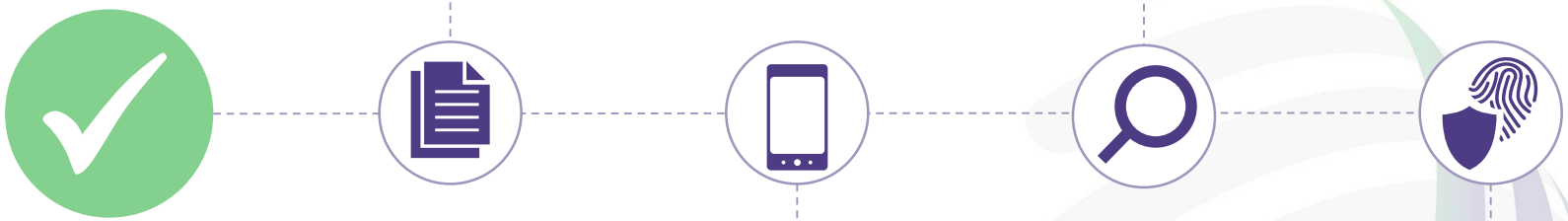
What's New

More Data Than Before

Additional data helps reduce friction during the authentication process.

Non-Payment Authentications

Identity verifications for card or token provisioning as well as account confirmations.



Additional Device Channels

Smart devices including mobile phones, tablets, televisions, and wearables can now be enabled with 3DS. Merchant-initiated transactions are also supported.

New Authentication Methods

Out-of-band and decoupled authentication methods to support more payment scenarios and checkout preferences.

US PAYMENTS FORUM

Key Benefits

Merchants

- Enables merchants to integrate authentication into their checkout process for both app- and browser-based implementations
- Minimizes checkout abandonment during authentication
- Ability to perform merchant-initiated authentications
- Helps reduce potential for fraud-related chargebacks
- Improved authorization rates

Issuers

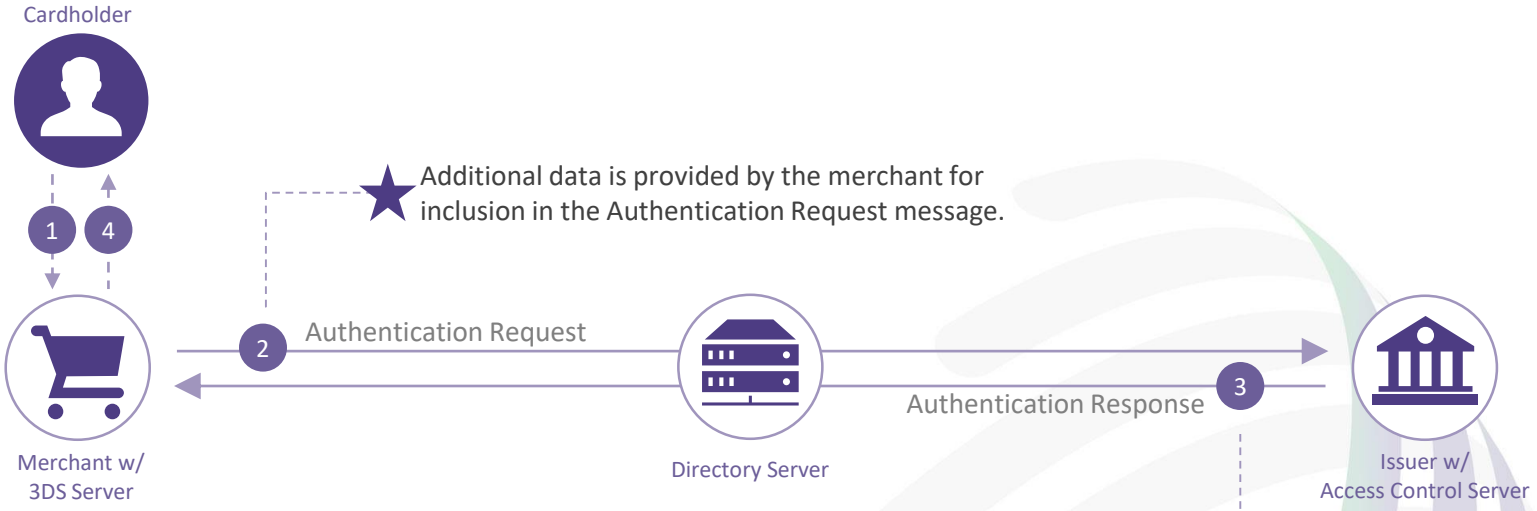
- Reduces risk of fraud
- Richer data exchange enables less friction during authentications
- Supports new devices and channels
- Flexibility to support a variety of authentication methods
- Encourages cardholders to make purchases using their preferred medium

Consumers

- Most authentications will be invisible to consumers
- Enhances online security
- Improved and consistent user experience

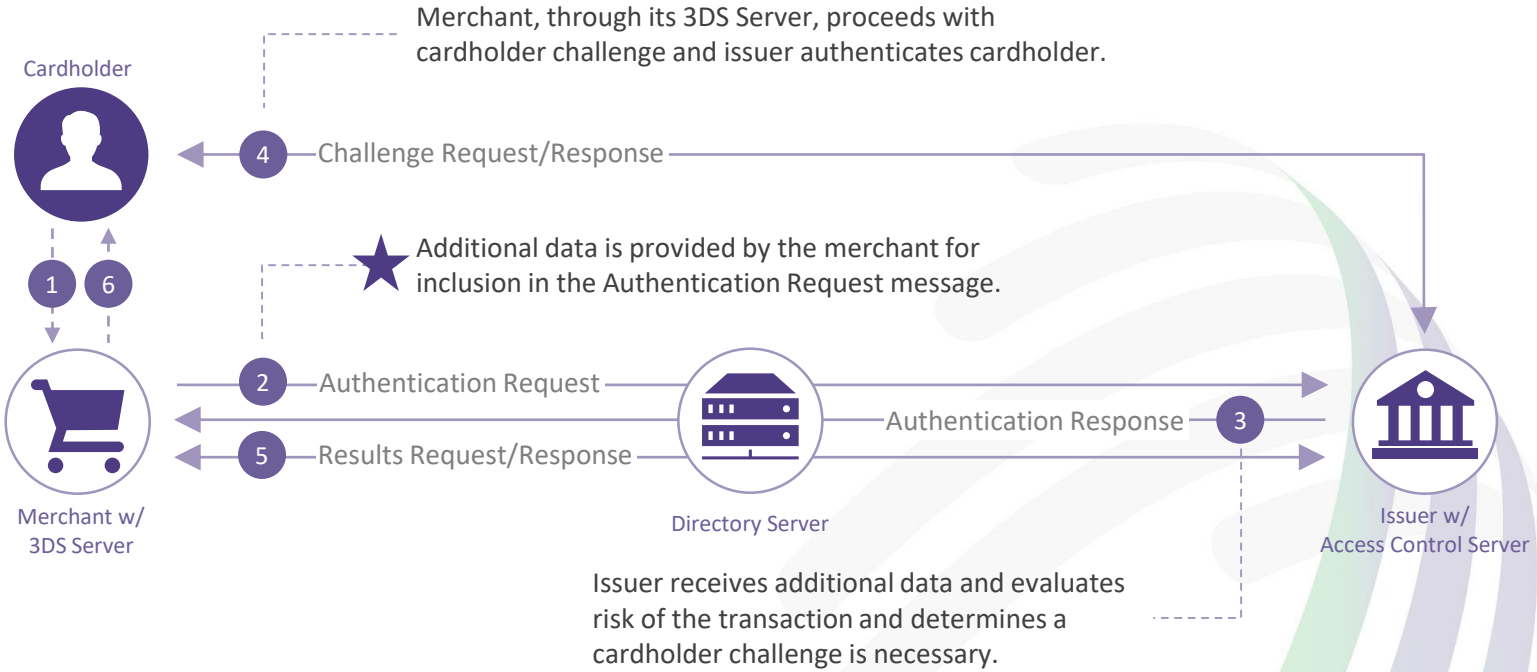
US PAYMENTS FORUM

Frictionless Flow



Issuer receives additional data and evaluates risk of the transaction. If the issuer determines the transaction to be low-risk and believes the transaction is legitimate, authentication may occur without cardholder interaction. Proof of authentication will be provided in the Authentication Response message.

Challenge Flow



EMV® 3-D Secure Data Elements

Ian Poole, Sr. Director, Global Product, CardinalCommerce

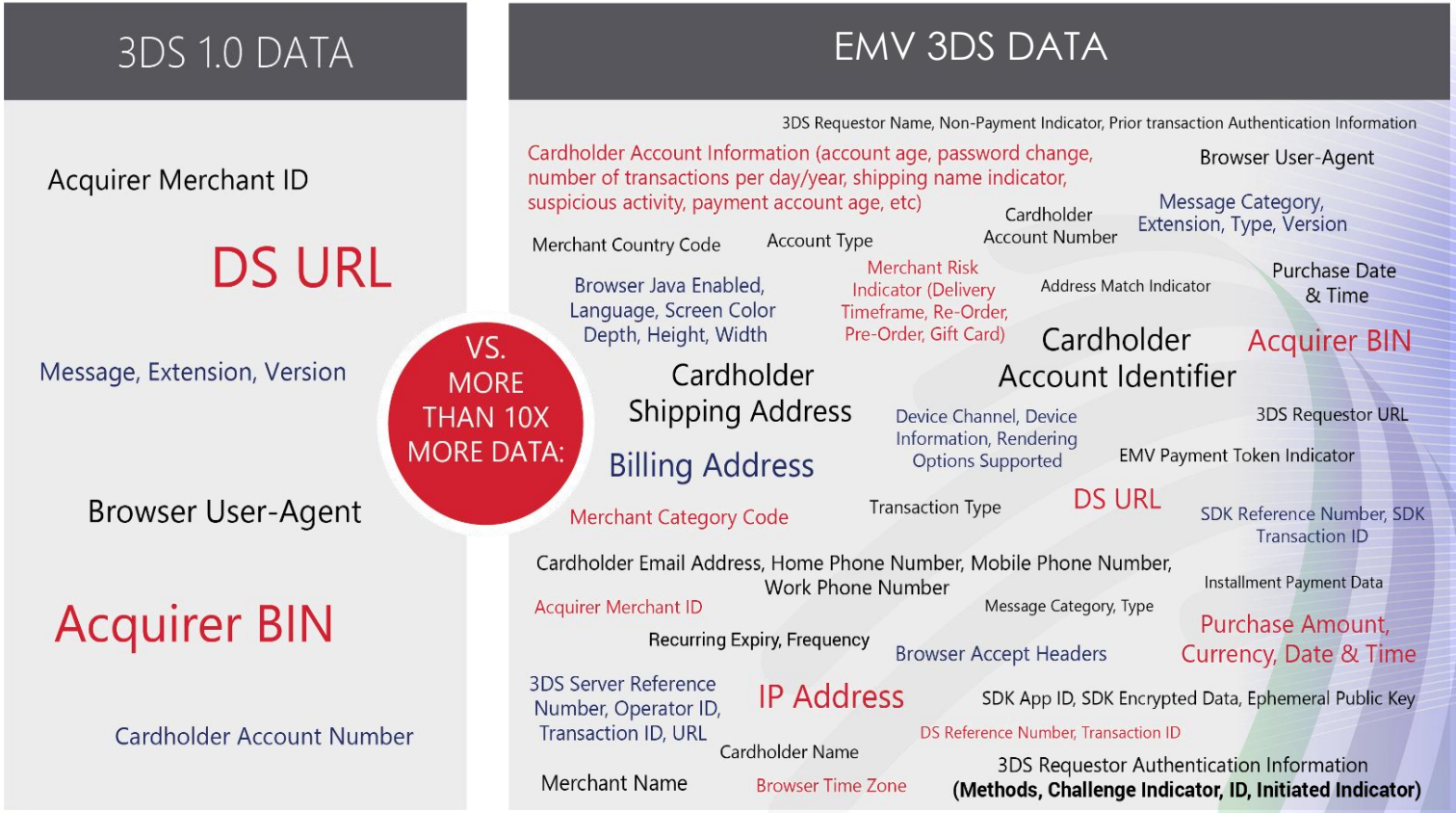
EMV® 3-D Secure Authentication Strategy

Moving towards dynamic, risk-based authentication

- Reduce false-declines while minimizing fraud loss
- Optimize the consumer experience
  - Mostly friction-free, introduction of biometrics, universal device usage
- Enable global interoperability
  - Regulatory smart for regional/country compliance
- Greater Data Exchange
  - Including non-payment, 3RI

Data Source for this document: EMVCo EMV® 3-D Secure Protocol and Core Functions Specification, 3-D Secure 2.1.0, 30 Oct 2017

More Data Shared between Stakeholders



US PAYMENTS FORUM

4 Types of Data

4

Device Data

3DS SERVER (formerly MPI)

DIRECTORY SERVER

ACCESS CONTROL SERVER (ACS)

Transaction & Consumer Data

1

Authentication Data

2

Merchant Data

3

US PAYMENTS FORUM

16

Data Type	Data Description	Data Requirement
Transaction & Checkout Page Data	• Contains required or conditional information gathered from the cardholder's checkout process with the merchant and transaction elements	Required / Conditional
Authentication Data	Merchant Authentication • Pertains to the use of non-3DS authentication which may be used in order for the cardholder to gain access to the merchant website, account or card on file details Prior Authentication: • Is data elements gathered to present on a new transaction, from an existing transaction with the same cardholder and PAN where EMV 3DS was applied	Optional
Merchant Data	Merchant Risk Info: • Data that only the merchant would be able to verify based on the current order details and utilized for risk analysis Cardholder Account Info: • Merchant specific account information on the cardholder related to the history or details of their account	Optional
Device Data	• Specific device information per channel like Native App iOS vs Native App Android, vs Browser	Required / Conditional

Transaction & Checkout Page Information

Action: Required

Cardholder Info	Account Number & Expiration Date, Billing: Address, City, Postal Code, State, Email, Mobile Phone, Cardholder Name, Shipping: Address, City, Country, Postal Code, State
Merchant Info	Merchant Name, URL, Country, MCC, Acquiring BIN/MID, 3DS Network Identifier
Transaction Info	Amount, Currency Code Transaction Type
Device Info	**Device Channel** (App, BRW, 3RI), **Browser**: Header, IP Address, Java Enabled, Language, Color Depth, Screen Height, Screen Width, Time Zone, User Agent, **App**: SDK Encrypted Data

US PAYMENTS FORUM

Authentication Data

Action: Optional

Merchant Authentication:

Merchants can convey to the issuer whether the cardholder logged in successfully or not to the merchant site, to help the issuer with their risk decision.

Authentication Method

- No authentication occurred – Guest Checkout
- Login using Merchant system credentials
- Login using Federated ID
- Login using FIDO authenticator

Authentication Date

- Date & Time when the authentication occurred **on the merchant's site**

Authentication Data

- Any data to document specifics of the authentication process that previously occurred

US PAYMENTS FORUM

Authentication Data (cont'd)

Action: Optional

Prior Authentication:

Passing previous EMV 3DS authentication that occurred on a cardholder transaction

Authentication Method	• Frictionless authentication occurred • Cardholder challenge occurred by ACS
Authentication Date	• Date & Time when the prior **EMV 3DS authentication** occurred on the merchant's site
Authentication Data	• Any data to document specifics of the authentication process that previously occurred • **ACS Transaction ID** to link the prior authentication

US PAYMENTS FORUM

Merchant Data

Action: Optional

Merchants can provide their own risk identifiers that can improve the scoring of a transaction with an issuer. Sharing this data frequently can build or validate consumer buying patterns leading to more frictionless authentication opportunities

Shipping & Delivery

- Ship Method Indicator
  - Ship to billing address, ship to another verified address on file, Ship to address different from Billing, Ship to store
- Delivery Email
- Delivery Timeframe
  - Electronic Delivery, Same day shipping, Overnight shipping, Two or more day shipping

Pre-Order/Re-Order

- Merchandise available, Future availability
- First time order, Reordered product

Gift Card

- Amount, Currency, Count

US PAYMENTS FORUM

Merchant Data (cont'd)

Action: Optional

Cardholder Account Info:

Merchants have the unique ability to collect data based on their historical relationship with the cardholder and their account at the merchant

Account Standing

- Account Age Indicator
- Account Creation Date
- Account Change Indicator, Change Date
- Account Password Change, Indicator, Date
- Ship Name Indicator
- Payment Account Indicator and Age

Shipping Usage

- Shipping Address usage & date
  - When address was first used

Transaction Counts

- Number of transactions within the last 48hrs
- Amount, Currency Code, Count

Fraud Activity

- Suspicious activity on account
- Account purchases and Add-Card attempts

US PAYMENTS FORUM

Device Data

Action: Required/Conditional

Browser-based

Device Channel (App, BRW, 3RI), Browser: Header, IP Address, Java Enabled, Language, Color Depth, Screen Height, Screen Width, Time Zone, User Agent, App: SDK Encrypted Data

Native App-based

Common: Platform, Device Model, OS Name, OS Version, Locale, Time zone, Advertising Id, Screen Resolution, Device Name, IP Address, Latitude, Longitude

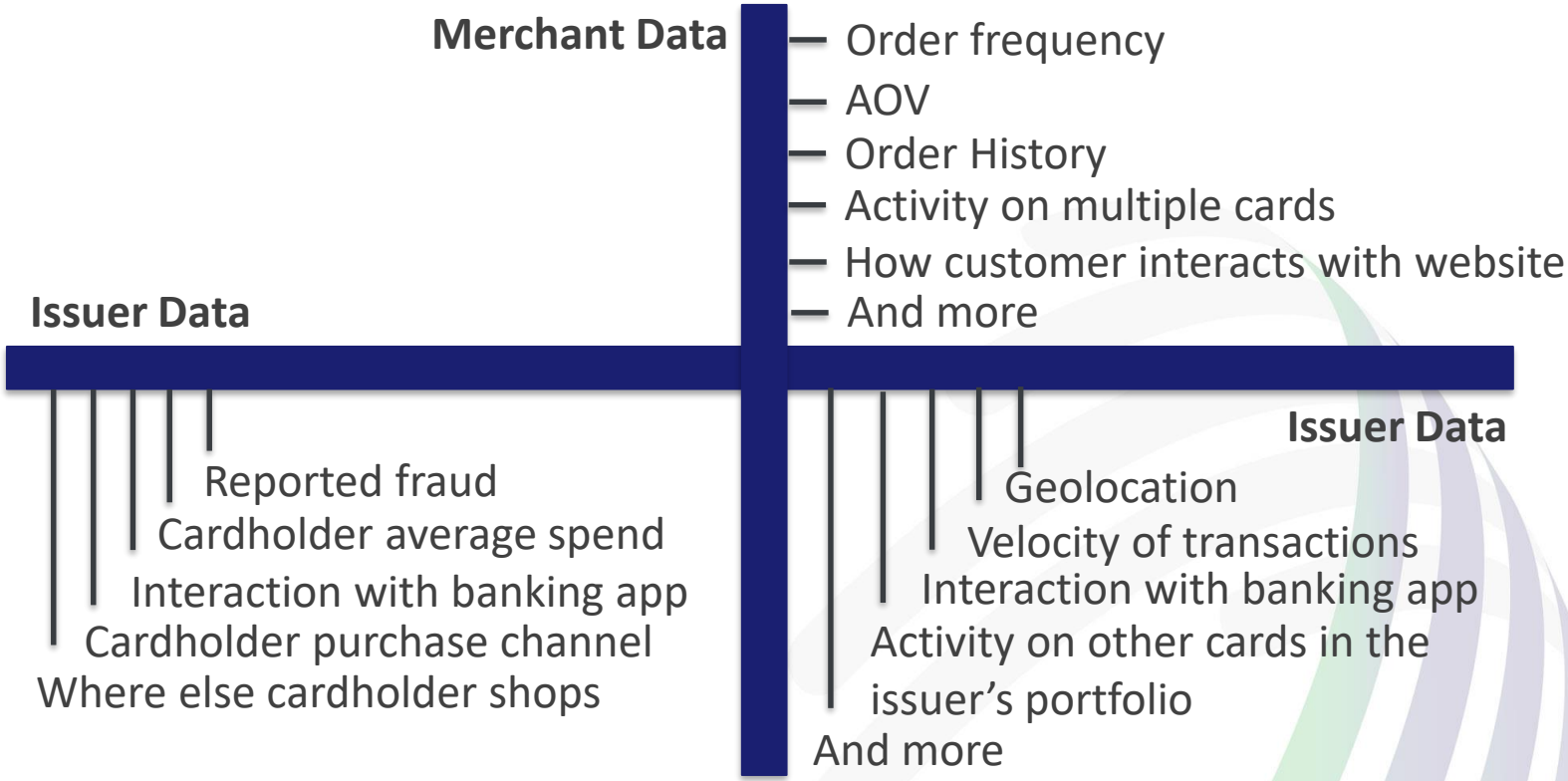
- *iOS:* 10+ fields like Family Names, System Font, Label Font Size, System Locale, Preferred Languages
- *Android:* 100+ fields like Subscriber Id, IMEI, Device Id, Network Country Code

Data Category Recap

DATA TYPE	DATA REQUIREMENTS
Transaction & Checkout Page Information	Required / Conditional
Authentication Data	Optional
Merchant Data	Optional
Device Data	Required / Conditional

US PAYMENTS FORUM

Imagine how powerful …



… if these data were shared

Q&A

US PAYMENTS FORUM

www.uspaymentsforum.org

U.S. Payments Forum

- **U.S. Payments Forum EMV 3DS Data Elements Project**
  - If you'd like to participate in the project, contact Cathy Medich, cmedich@uspaymentsforum.org
- **March U.S. Payments Forum Member Meeting and 2019 Payments Summit**, Mar. 11-14, Phoenix, AZ
  - **Mar. 11-13 – Forum Member Meeting**: roundtables, SIGs, working committee and birds-of-a-feather sessions
  - **Mar. 12-14 – 2019 Payments Summit**: multiple tracks covering all things payments, including FinTech, EMV chip technology, mobile wallets, NFC, contactless, open transit systems and more
- Other resources available at: www.uspaymentsforum.org

Randy Vanderhoof, rvanderhoof@uspaymentsforum.org
Kristy Cook, kristy.cook@target.com
Michael Horne, michael.horne@aexp.com
Ian Poole, ipoole@cardinalcommerce.com
Cathy Medich, cmedich@uspaymentsforum.org

US PAYMENTS FORUM

www.uspaymentsforum.org