

How Digital Identity Will Power the Next Wave of Improvements to the Checkout Experience

Dan Macias – VP, North America Products, Visa

Matt Charpentier – VP, Authentication and Identity, Visa



Notices and Disclaimers

Third Party Marks: All brand names and logos are the property of their respective owners, are used for identification purposes only, and do not imply product endorsement or affiliation with Visa.

Forward – Looking Statements: This presentation contains forward-looking statements within the meaning of the U.S. Private Securities Litigation Reform Act of 1995 that relate to, among other things, our future operations, prospects, developments, strategies, business growth and financial outlook. Forward-looking statements generally are identified by words such as "believes," "estimates," "expects," "intends," "may," "projects," "could," "should," "will," "continue" and other similar expressions. All statements other than statements of historical fact could be forward-looking statements, which speak only as of the date they are made, are not guarantees of future performance and are subject to certain risks, uncertainties and other factors, many of which are beyond our control and are difficult to predict. We describe risks and uncertainties that could cause actual results to differ materially from those expressed in, or implied by, any of these forward-looking statements in our filings with the SEC. Except as required by law, we do not intend to update or revise any forward-looking statements as a result of new information, future events or otherwise.

As Is: Case studies, comparisons, statistics, research and recommendations are provided "AS IS" and intended for informational purposes only and should not be relied upon for operational, marketing, legal, technical, tax, financial or other advice. Visa Inc. neither makes any warranty or representation as to the completeness or accuracy of the information within this document, nor assumes any liability or responsibility that may result from reliance on such information. The presentation contained herein is not intended as investment or legal advice, and readers are encouraged to seek the advice of a competent professional where such advice is required.

Best Practice: These materials and best practice recommendations are provided for informational purposes only and should not be relied upon for marketing, legal, regulatory or other advice. Recommended marketing materials should be independently evaluated in light of your specific business needs and any applicable laws and regulations. Visa is not responsible for your use of the marketing materials, best practice recommendations, or other information, including errors of any kind, contained in this presentation. Issuers are solely responsible for their installment programs.

Product/Ideas in Development: This presentation is intended for illustrative purposes only. It contains depictions of a product currently in the process of development and should be understood as a representation of the potential features of the fully-deployed product. The final version of this product may not contain all of the features described in this presentation.



IDENTITY & PAYMENTS
SUMMIT

~\$ 9 B

Forecasted e-Commerce fraud in
the U.S. by 2026¹

Sources: [1] Datas Insights, CNP Fraud and the Role of 3-D Secure, Nov 2023. [2] J.P. Morgan article <https://www.jpmorgan.com/insights/payments/analytics-and-insights/cnp-fraud-prevention-combat-chargebacks>



~\$13 B

Forecasted e-Commerce fraud in
the U.S. by 2026¹

Sources: [1] Datas Insights, CNP Fraud and the Role of 3-D Secure, Nov 2023. [2] J.P. Morgan article <https://www.jpmorgan.com/insights/payments/analytics-and-insights/cnp-fraud-prevention-combat-chargebacks>



~\$13 B

Forecasted e-Commerce fraud in
the U.S. by 2026¹

1 X higher

Impact of declining a good customer is
estimated to be multiples more than
fraud losses²

~\$13 B

Forecasted e-Commerce fraud in
the U.S. by 2026¹

3 X higher

Impact of declining a good customer is
estimated to be multiples more than
fraud losses²

50%

Of Visa's card-not-present fraud globally happens right here in the U.S.

Source: Visa Risk Datamart, Visa Processed Volume + Collections, 1Q'22. Visa Proprietary.



70%

Of Visa's card-not-present fraud globally happens right here in the U.S.

Source: Visa Risk Datamart, Visa Processed Volume + Collections, 1Q'22. Visa Proprietary.



With limited data and insights, issuers are doing their best to balance fraud capture vs false positive decline...

...with less than optimal results

Maximize
Fraud Capture Rate



CNP Fraud Rates are
5X higher
than those in CP¹

Source: [1] Visa Risk Datamart, NA, YE'1Q23, [2] VisaNet Data, NA, FY23, approval rate based on deduped authorizations. Visa Proprietary.



With limited data and insights, issuers are doing their best to balance fraud capture vs false positive decline...

...with less than optimal results

Maximize
Fraud Capture Rate

Minimize
False Positive Ratio



CNP Fraud Rates are
5X higher
than those in CP¹

CNP Approval Rates
~600 bps lower
than those in CP²

Source: [1] Visa Risk Datamart, NA, YE'1Q23, [2] VisaNet Data, NA, FY23, approval rate based on deduped authorizations. Visa Proprietary.



A two-pronged approach to identity is how we address those challenges



Probabilistic

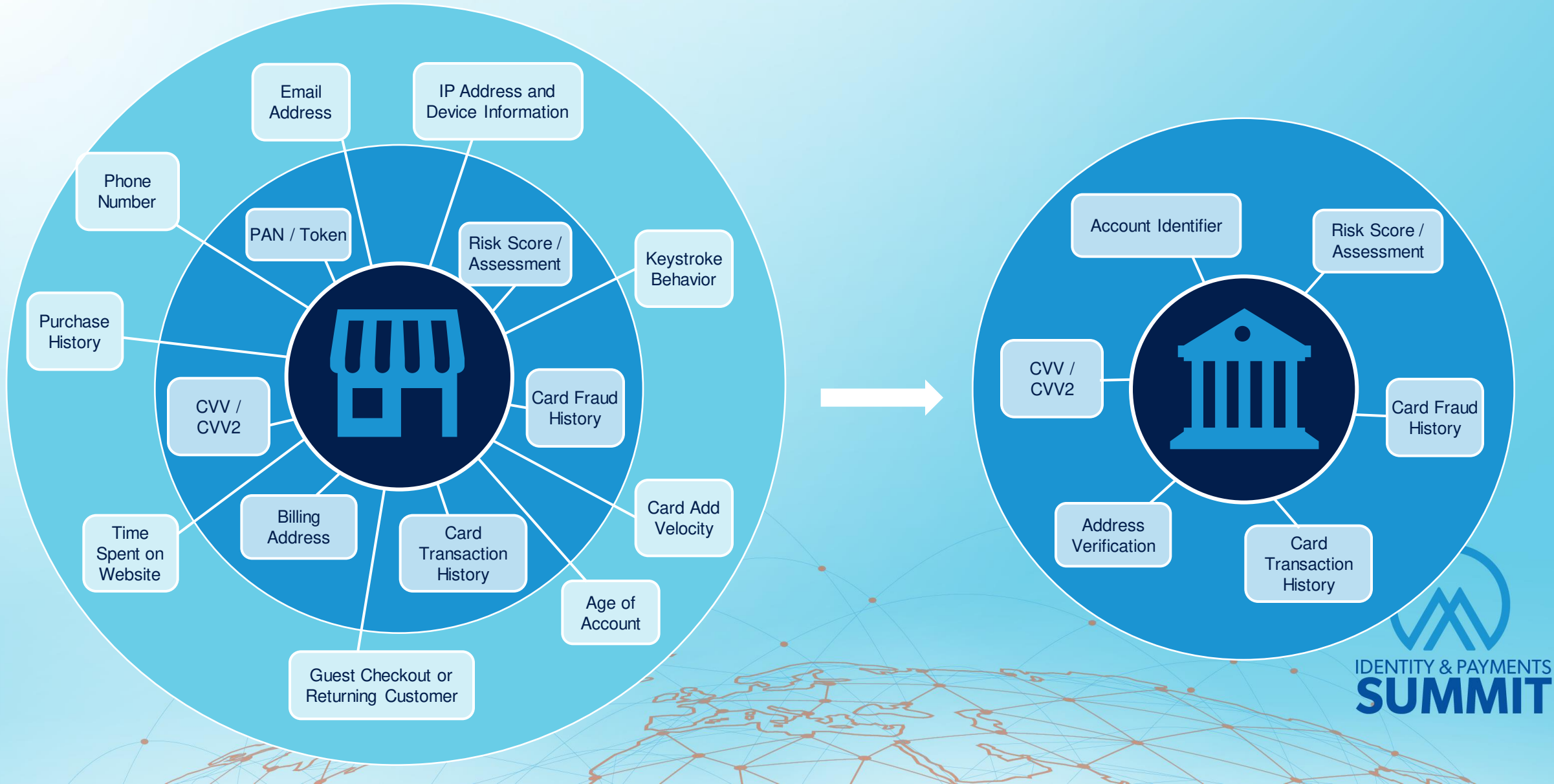
More (and better) data exchange in the ecosystem



Deterministic

Better authentication methods


Many valuable insights on the customer and transaction are siloed in the ecosystem



With enhanced data sharing from merchants, issuers can better split risk and more confidently approve good transactions while declining bad transactions.

Performance improvement using enhanced data is greatest on medium to high risk (~40%) transactions

Approval Rate
+ 427 bps 
vs. 84.6% baseline

Fraud Rate
- 4.1 bps 
vs. 28 bps baseline

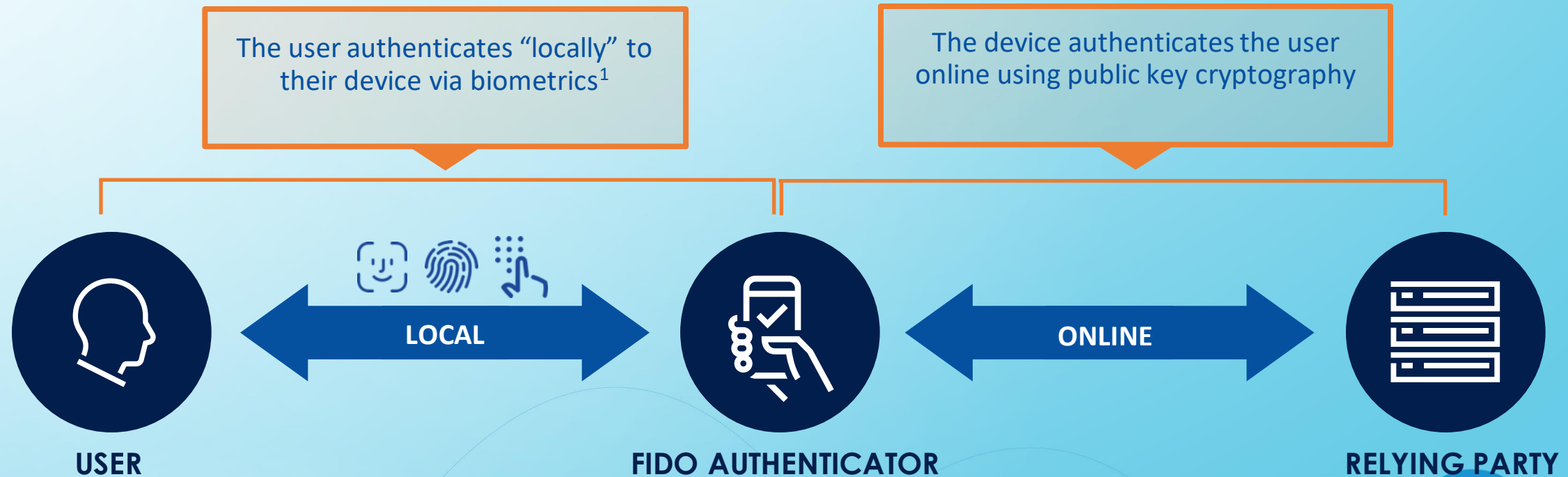
*Visa Data Only
in partnership with*

adyen

 **Square**

What is FIDO and how does it work?

Fast Identity Online (FIDO) is a global authentication standard based on public key cryptography. It replaces legacy forms of authentication such as passwords or SMS OTPs with simple to use, phishing resistant authentication credentials called passkeys.

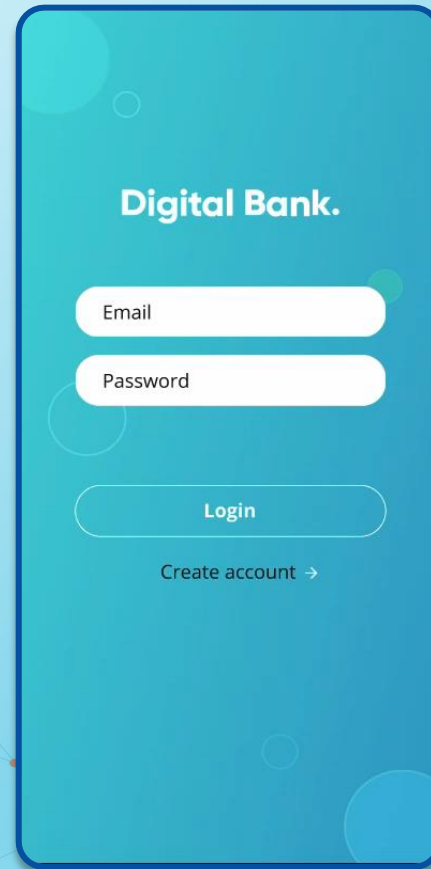


Source: FIDO Alliance Presentation
1: authentication can happen via other means (e.g.: PIN)

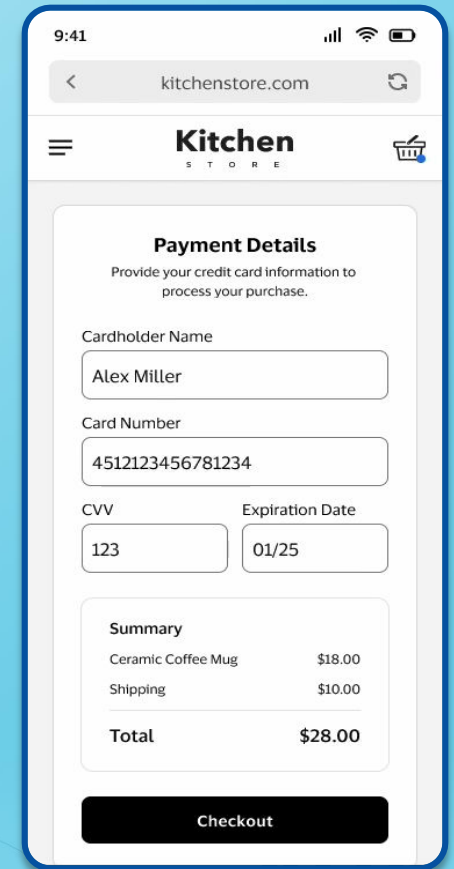
FIDO for payment authentication



Passkey registration



Passkey payment authentication



Why FIDO is good for payments

Fraud & Approval Rates

When biometric authentication methods are used for 3-D Secure transactions we see:

- **75%+ reduction in reported fraud rate** (global average)¹
- **4%+ increase in approval rates** (global average)¹

User Experience

No need to remember passwords or use SMS OTPs

Consistent & familiar user experience – same method as how users unlock their devices everyday

Enables streamlined checkout process & reduced purchase abandonment

Broadly Accessible

Standards-based protocol

All major OS providers and 88% of web browsers support FIDO authentication natively ²

Estimated 4 billion consumer devices support FIDO authentication²

Security & Privacy

Provides verifiable proof of authentication

Phishing resistant credentials

Biometric data never leaves the user's personal device ³

¹ Source: Visa data from Oct 2022 – Oct 2023, stats represent a percent change in fraud and approval rates. Visa Proprietary.

² FIDO Alliance: <https://fidoalliance.org/fido-alliances-new-user-experience-guidelines/>

³ FIDO Alliance Privacy Principles: <https://fidoalliance.org/fido-authentication-2/privacy-principles/>

Thank you



IDENTITY & PAYMENTS
SUMMIT