


Changing Browsers and the Impact on Payments



The World Wide Web Consortium (W3C) is an international community that develops open standards to ensure the long-term growth of the Web.


Today's Agenda

- * **What's driving our work**
- * Streamlining e-commerce authentication to increase conversions
- * New signals to help with fraud mitigation
- * Returning user recognition

E-commerce trends

- * E-commerce ↑
- * Mobile ↑
- * Fraud ↑
- * User journey must be quick, secure
- * Custom experiences important

Why EMV 3DS?



More and more consumers are shopping online using a variety of devices.

E-commerce fraud is a growing challenge for businesses to manage.

Consumers expect a secure, quick and convenient e-commerce checkout experience.

\$800 billion*
Projected total of U.S. e-commerce sales in 2020, an increase of more than 30% year-over-year.

\$6.4 billion*
Projected U.S. e-commerce fraud losses in 2021.

\$443 billion*
Projected U.S. e-commerce losses due to false declines in 2021.

20%*
Projected percentage of U.S. retail sales that are online by 2024.

77%
Percentage of surveyed U.S. consumers that indicated keeping payment information safe is one of the most important factors when choosing how to pay.

"Given the rapid growth of e-commerce globally, merchants must engage with the digital channels or risk following the path of the dinosaurs. But they also have to manage digital channel activity with finesse to increase sales while improving security in an environment in which threats are ever-growing and consumers demand an easy, quick, and convenient checkout experience."

*U.S. Retail E-Commerce Sales, 2018-2024 (emarketer)

*The E-Commerce Conundrum: Balancing False Declines and Fraud Prevention (Aite Group)

*Deloitte U.S. Consumers Credit Card Payments Survey (Deloitte Insights)

Authentication trends

- * Increasing SCA regulation

- * EU, UK, India, ...

- * User expectations evolving

- * Half (47%) of consumers surveyed say they are more likely to sign up to an app or online service if a company offers Multi-factor Authentication (MFA)."
—Auth0 Survey (2021)

- * FIDO2 ubiquitous

- * On billions of devices

- * Coordinated effort by platform providers to replace passwords with FIDO (“passkeys”)



But friction can lead to failure

See *Microsoft report on 3DS performance discussed at W3C's TPAC 2022 (Sep)*

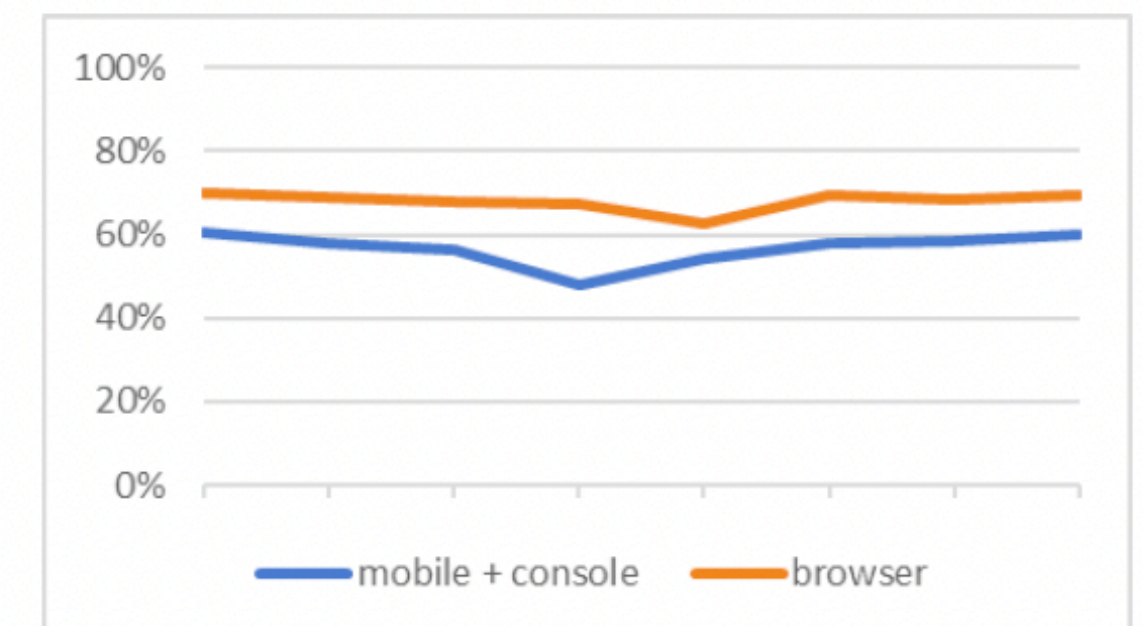
- * Authentication success rate “too low”
- * Abandonment “too high”
- * Challenge rates “too high”
- * Challenge success “too low”

“Approval rates improve when challenge succeeds, but purchase **conversion is net negative with SCA.**”

Challenge success is too low

	mobile + console	web
EU ex UK	57%	68%
UK	67%	72%

Mobile + console performance remains poor relative to web.



Privacy trends

* Growing privacy regulation

* *By year-end 2024, Gartner predicts that 75% of the world's population will have its personal data covered under modern privacy regulations. — [Gartner report](#)*

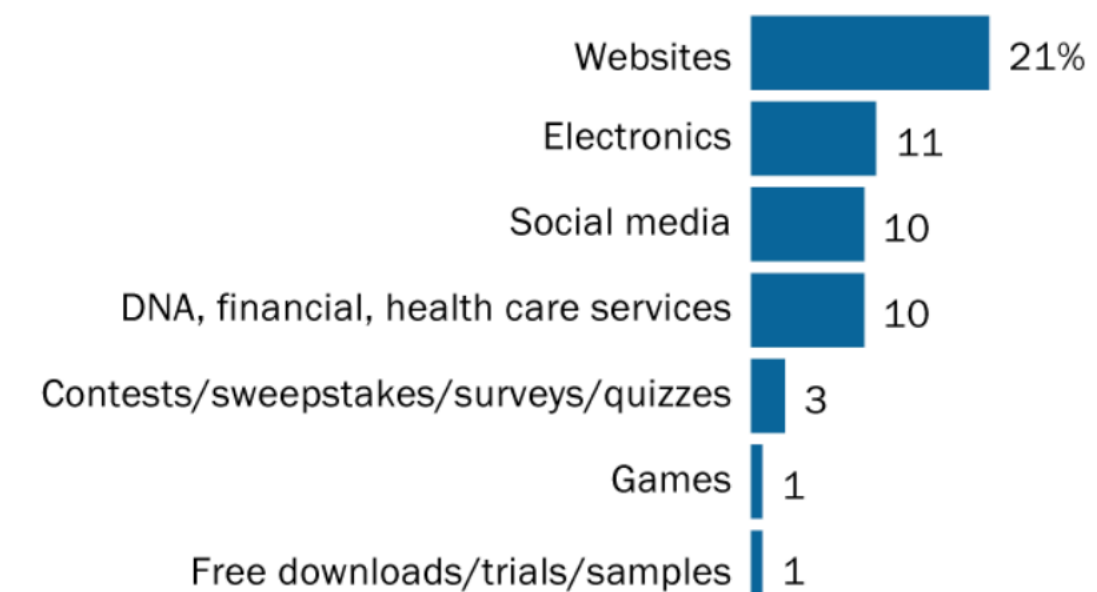
* Changing user expectations

* *Half of Americans have decided not to use a product or service because of privacy concerns. — [Pew Report](#)*

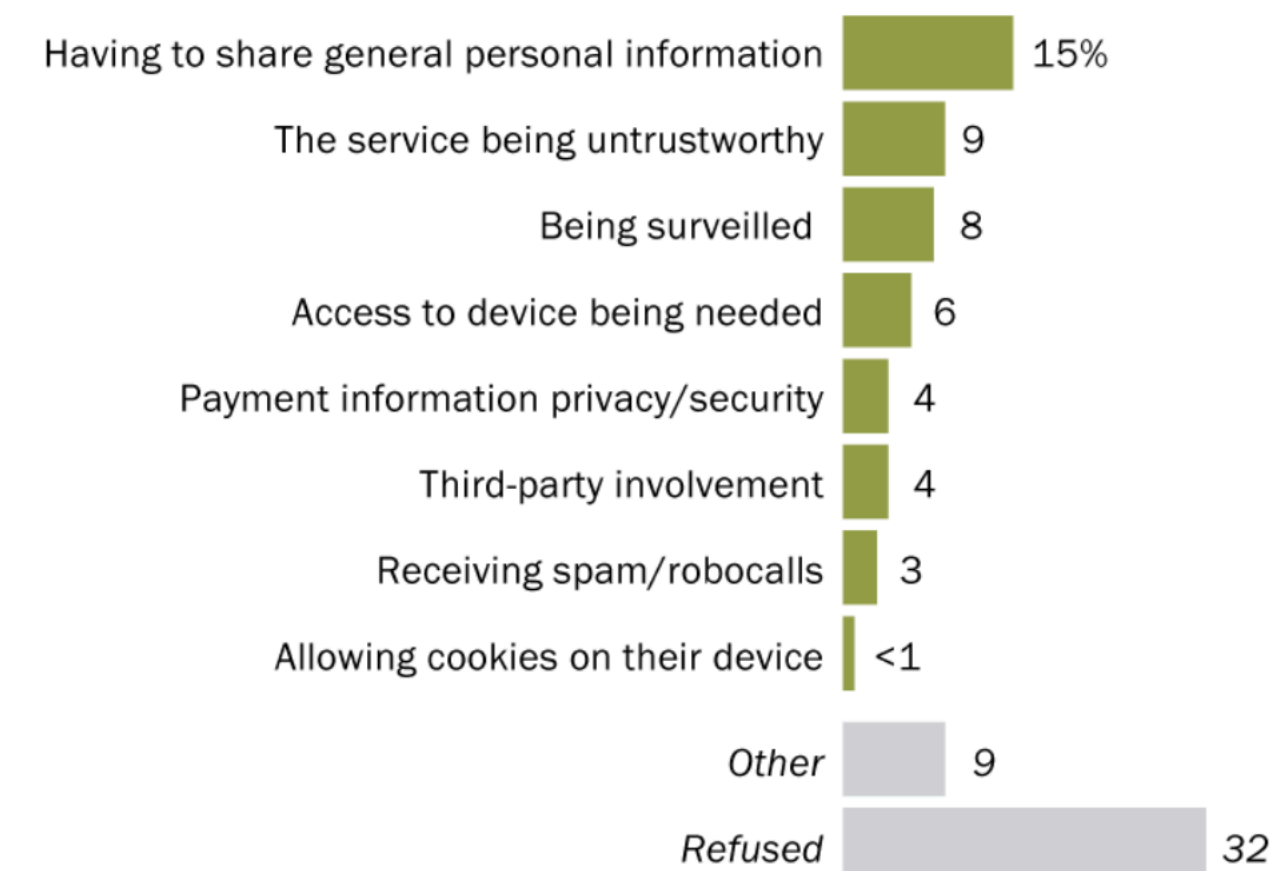
Americans give up websites, electronics and social media to avoid sharing personal information

Among the 52% who say they recently decided NOT to use a product or service because they were worried about how much personal information would be collected about them, % who describe a recent situation where they ...

Decided not to use ___ over concerns about how much personal information would be collected



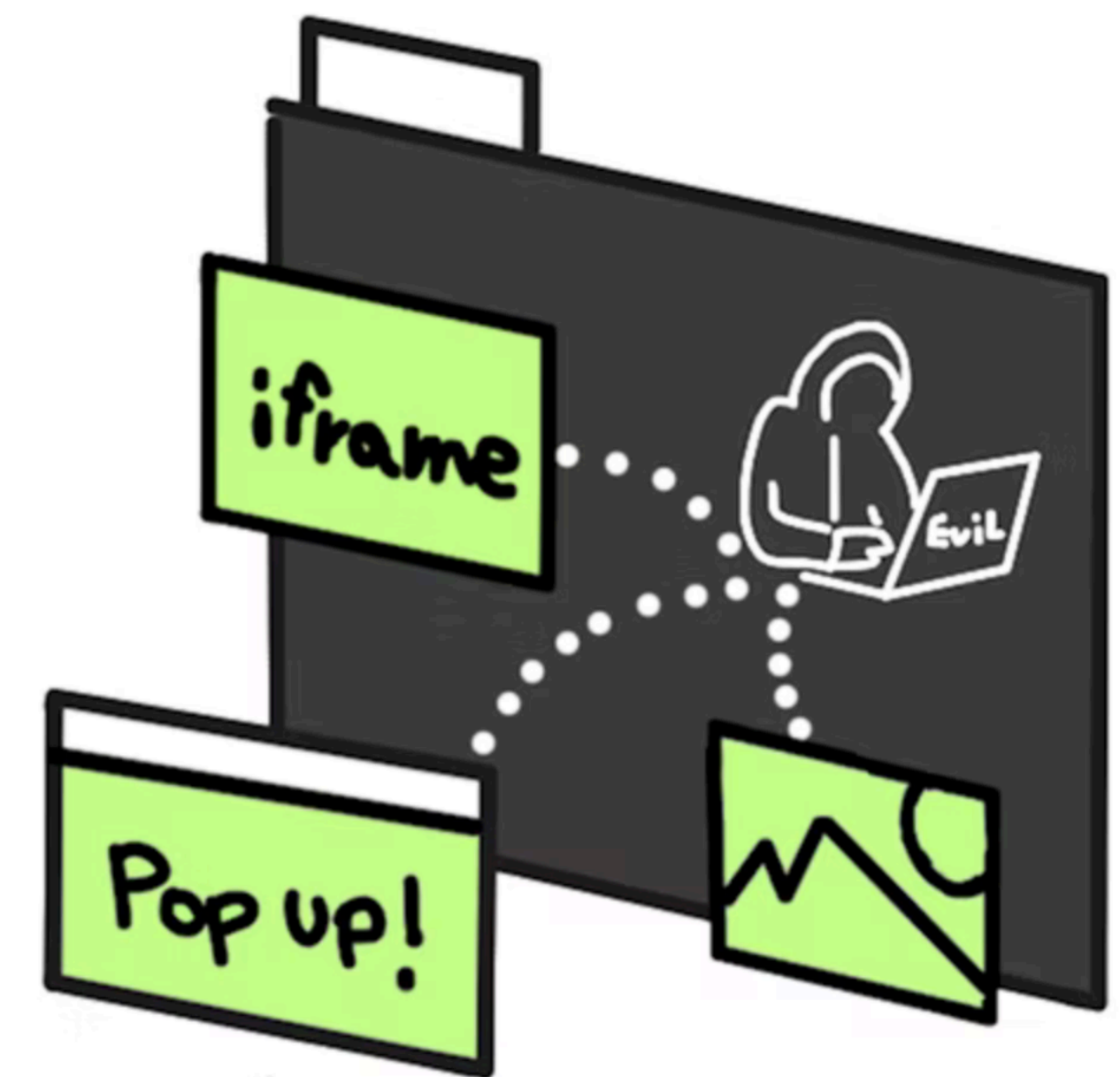
Found that ___ was problematic



Source: Pew Report on Privacy

Web security and privacy - the origin model

- * Browser's trust model based primarily on the domain (or "origin")
 - * <https://merchant.com/> and <https://psp.com/> are different origins
- * Browsers mediate exchanges across trust boundaries
- * But cross-origin content is common on the Web
 - * Ads, analytics, media, scripts, embedded content (via **iframe**).
 - * Payment service providers often operate from iframes
- * Server-side terminology
 - * First party (1p): Origin the user visits
 - * Third party (3p): Anyone not the first party or user, thus:
"cross-origin iframe" => third party



How Browsers Mediate Exchanges is Changing

* Webkit Intelligent Tracking Prevention (ITP): Safari



* Chromium Privacy Sandbox: Chrome, Edge, Opera, Brave, Samsung Internet



* Firefox Enhanced Tracking Protection: Firefox, Tor



Impact of browser changes on payments

- * Inability to recognize returning users could mean more UX friction, and more difficulty creating a custom experience
- * Fraud mitigation that relies on current signals will no longer be effective, further raising challenge rates
- * The Web has embraced FIDO authentication; key is to raise challenge success rates

EMV® 3-D Secure Protocol and Core Functions Specification v2.3.1.0
3-D Secure Data Elements

can be obtained by 3DS software provided to the 3DS Requestor 3DS Server to ensure that the data is not altered or hard-coded a Cardholder Browser for each transaction are:

- Browser Accept Headers
- ~~Browser IP Address~~
- Browser Java Enabled
- ~~Browser Language~~
- Browser Screen Color Depth
- Browser Screen Height
- Browser Screen Width
- Browser Time Zone
- ~~Browser User-Agent~~

Refer to Table A.1 for data element specifications.

Notes:

- *These changes affect 3DS Requestor and ACS as well (via methodURL).*
- *Private browsing further reduces signal availability*

“Approval rates improve when challenge succeeds, but purchase conversion is net negative with SCA.”

What can the browser do to help?

A word on how W3C works

- * Exploratory discussions (e.g., Workshops, Interest Groups)
- * Technology incubation (e.g., in Community Groups) and experimentation (e.g., pilot implementations)
- * Best practice integration (accessibility, privacy, security, i18n, architecture)
- * Industry coordination and adoption (e.g., **Web Payment Security Interest Group**)
 - * Bilateral discussions in parallel (e.g., alignment between Web Authentication and CTAP (FIDO Alliance))
- * Standardization (in a Working Group); interoperability (e.g., test suites)
- * Maintenance (e.g., versioning); education (e.g., W3Cx)

Web Payment Security IG Participants

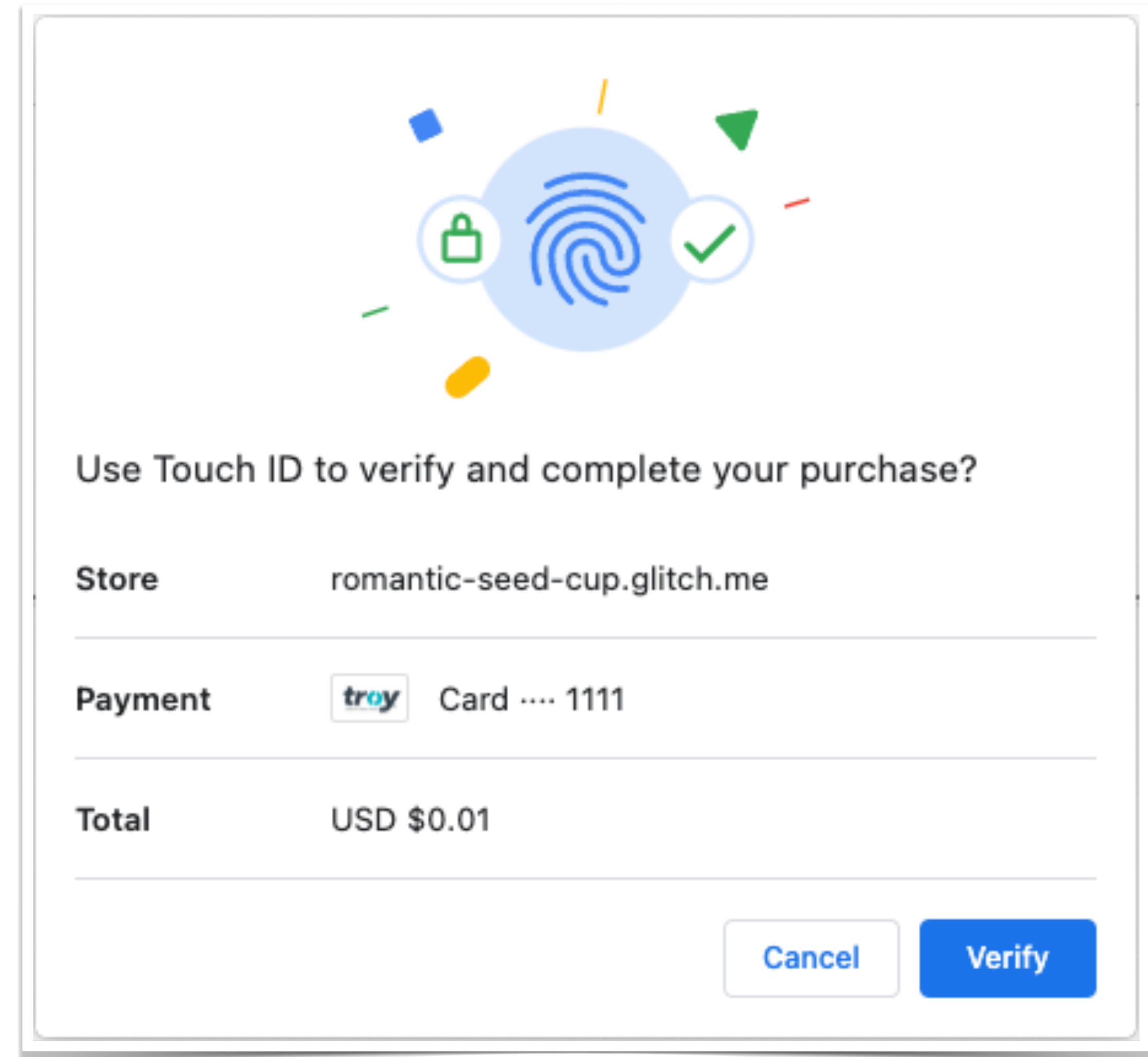
- * Aetna
- * Airbnb
- * Alibaba
- * American Express
- * ASSA ABLOY AB
- * Bank of America
- * Banksly
- * Brave Software
- * Canton Consulting
- * Capital One
- * The Clearing House
- * Conexus
- * Discover Financial Services
- * Entersekt
- * Federal Reserve Bank of Minn.
- * FEITIAN
- * FIME
- * Gemalto
- * Giesecke & Devrient
- * Google
- * Huawei
- * Infineon
- * ISO 20022 RA
- * JCB
- * JP Morgan Chase
- * KDDI
- * Knowbility
- * Lenovo
- * LogMeIn
- * Mastercard
- * Merchant Advisory Group (MAG)
- * Microsoft
- * Netflix
- * mSignia
- * Nok Nok Labs
- * Onespan
- * OpenID Foundation
- * PayPal
- * Ping Identity
- * Ripple
- * SSenStone
- * Shopify
- * SK Telecom
- * Stripe
- * TTA
- * Thales Group
- * UnionPay
- * Verizon
- * VinCSS
- * Visa
- * WebComm Technology
- * Who Are You Holdings
- * Worldline
- * Worldpay / FIS
- * Yahoo
- * Yubico

Today's Agenda

- * What's driving our work
- * **Streamlining e-commerce authentication to increase conversions**
- * New signals to help with fraud mitigation
- * Returning user recognition

Secure Payment Confirmation (SPC)

- * FIDO fine-tuned for payments
- * User can authenticate in merchant environment (without redirect, bank app, or bank code in page)
- * Output: cryptographic evidence of user consent to transaction



See: Adyen Registration & Authentication

Stripe Pilot: SPC versus OTP (within 3DS)

- * Conversions: **increased 8%** with SPC
- * Authentication: **over 3x faster** with SPC
- * Fraud: Negligible (for both SPC and OTP)

See Stripe experimental findings

SPC Status

- * Web Payments WG has stabilized version 1 specification
- * Browser support
 - * Deployed in some Chromium browsers (Chrome, Edge) on MacOS and Windows
 - * Chrome on Android anticipated January 2023. **Note:** Interest expressed in extending SPC to Android native apps.
 - * Ongoing discussions with other browser vendors
- * Pilots
 - * Stripe currently doing second pilot
 - * Adyen and Airbnb poised for pilot
- * Protocol integrations
 - * Integrated into EMV® 3DS 2.3.1
 - * Ongoing discussions with other payment and authentication flows (e.g., open banking)

FIDO2 / SPC Comparison

* FIDO and SPC

- * An origin can create credential in first party context (the “relying party”)
- * That origin can use it for authentication either in first party or third party context.
- * That origin can validate the results cryptographically.

* SPC-only — tweaks for payments flows

- * Built-in browser dialog displays transaction data for user consent
- * An origin can create credential in third party context.
- * Any origin can use it (with permission) to initiate authentication ceremony in first party or third party context.



SPC in 3DS: Issuer-initiated

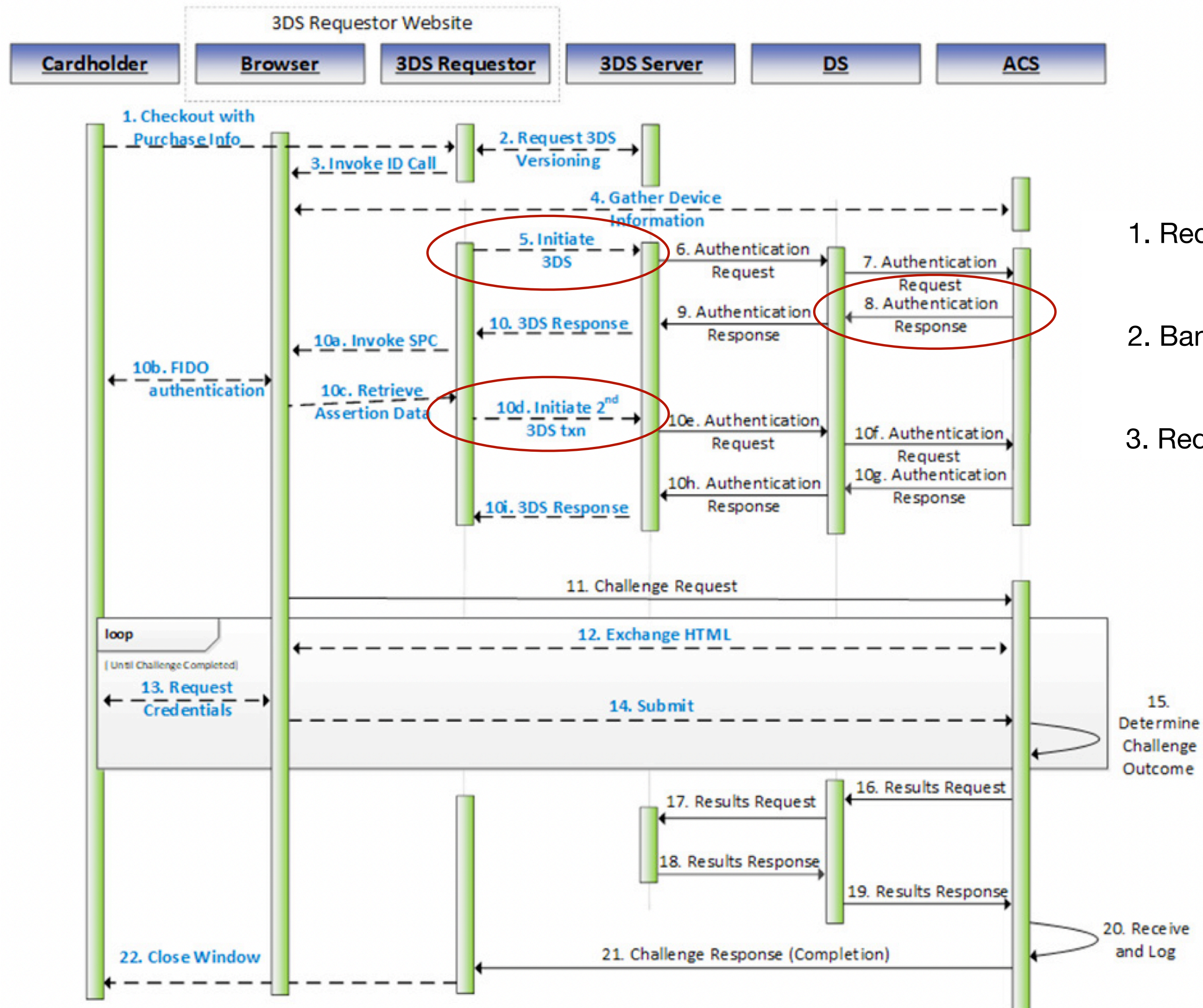
Creator of Credential	3DS Flow	Initiated by	Validated by	Note
Issuer	Challenge	Issuer	Issuer	Described in 3DS 2.3.1

See Modirum ACS demo with SPC

SPC in 3DS: Requestor-initiated

Creator of Credential	3DS Flow	Initiated by	Validated by	Note
Merchant/PSP	Frictionless	Merchant/PSP	Merchant/PSP	Delegated authentication. See EMVCo/FIDO Note " <u>FIDO Authentication and EMV 3-D Secure – Using FIDO for Payment Authentication</u> ". SPC includes transaction dialog.
Issuer	Challenge	Merchant/PSP	Issuer	Described in 3DS 2.3.1

3DS Flow: Requestor-initiated, issuer-validated



1. Requestor: "Here's transaction info; I can do SPC"
2. Bank: "Here are known credentials and a challenge"
3. Requestor: "Here are results for your validation"

Note: Dashed arrows are not part of the 3-D Secure 2.0 protocol but are shown for clarity.

Benefits of SPC “Decoupling”

- * User can stay in current merchant context
- * User can stay in current device context
 - * *No need to retrieve phone for OTP or native bank app, which might fail if phone off or unavailable*
- * Bank can validate results based on its own challenge
- * Promotes scale: **Register once, authenticate everywhere** (merchants)

Bigger Picture of FIDO/SPC Scale Efforts

	SPC	FIDO2
Reuse login credentials for payment use cases	FIDO Extension (temporary)	“Cross-origin bit” in CTAP
Reuse credential cross-browser		Discoverable credentials
Support more user experiences (without redirect)	Decouple authn ceremony from validation in iframe	Get() via iframe
Reuse phone credential with other devices		Hybrid/caBLE
Reuse a credential with other devices		Passkeys
Reuse a credential on different backends	Seeking more integrations in multiple payments protocols (card and others)	

Agenda

- * What's driving our work
- * Streamlining e-commerce authentication to increase conversions
- * **New signals to help with fraud mitigation**
- * **Returning user recognition**

Chromium view of fraud mitigation

* Replacing Functionality Served by Cross-site Tracking

- * Ad conversion measurement
- * Ads targeting
- * **Federated login**
- * SaaS embeds, third party CDNs

* Turning Down Third-Party Cookies

- * **Removing 3p cookies**

* Mitigating workarounds

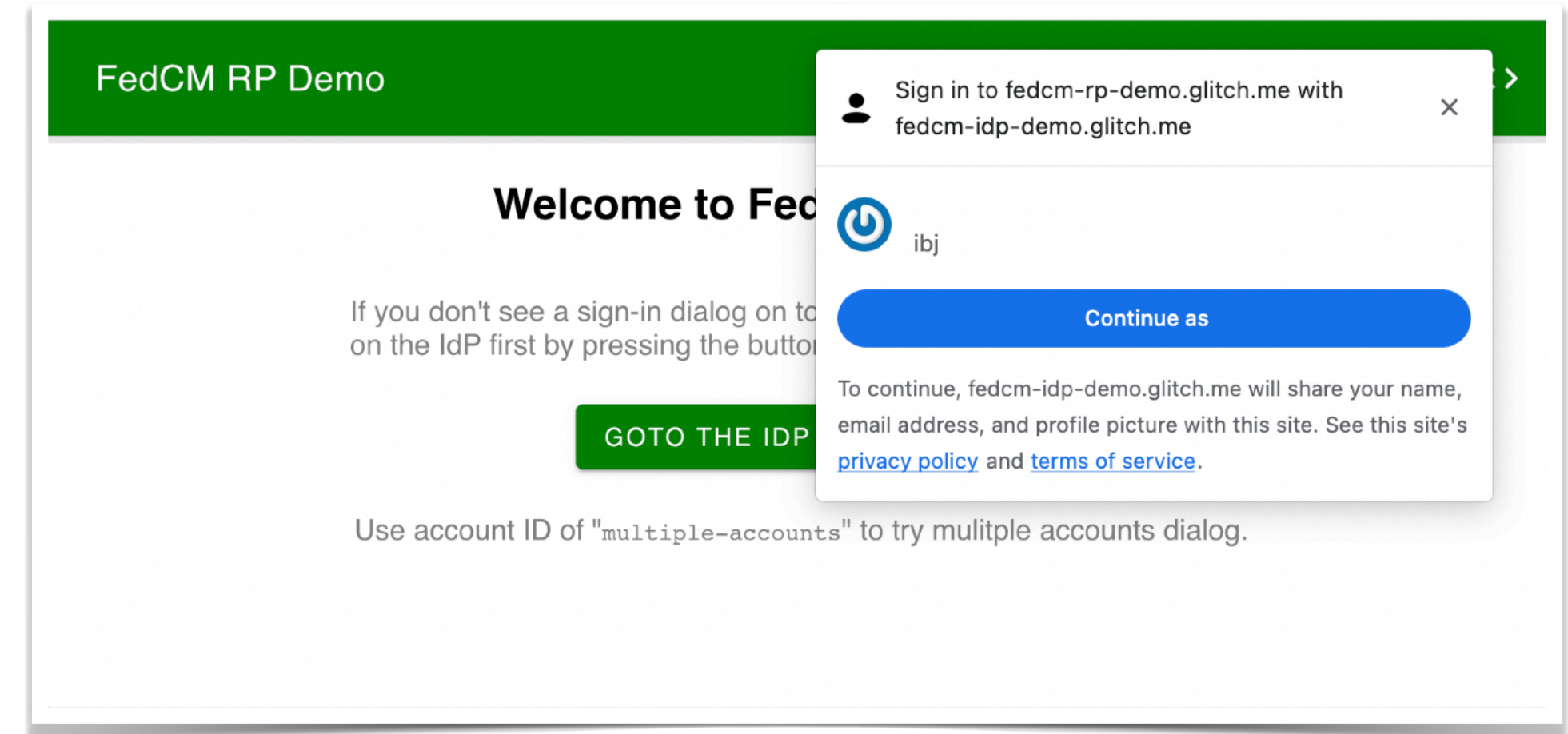
- * **Fingerprinting** (e.g., removing info from client side language, IP address, user agent string, device state, etc.)
- * Cache inspection
- * **Navigation tracking**
- * Network level tracking

How will emerging techs improve payments?

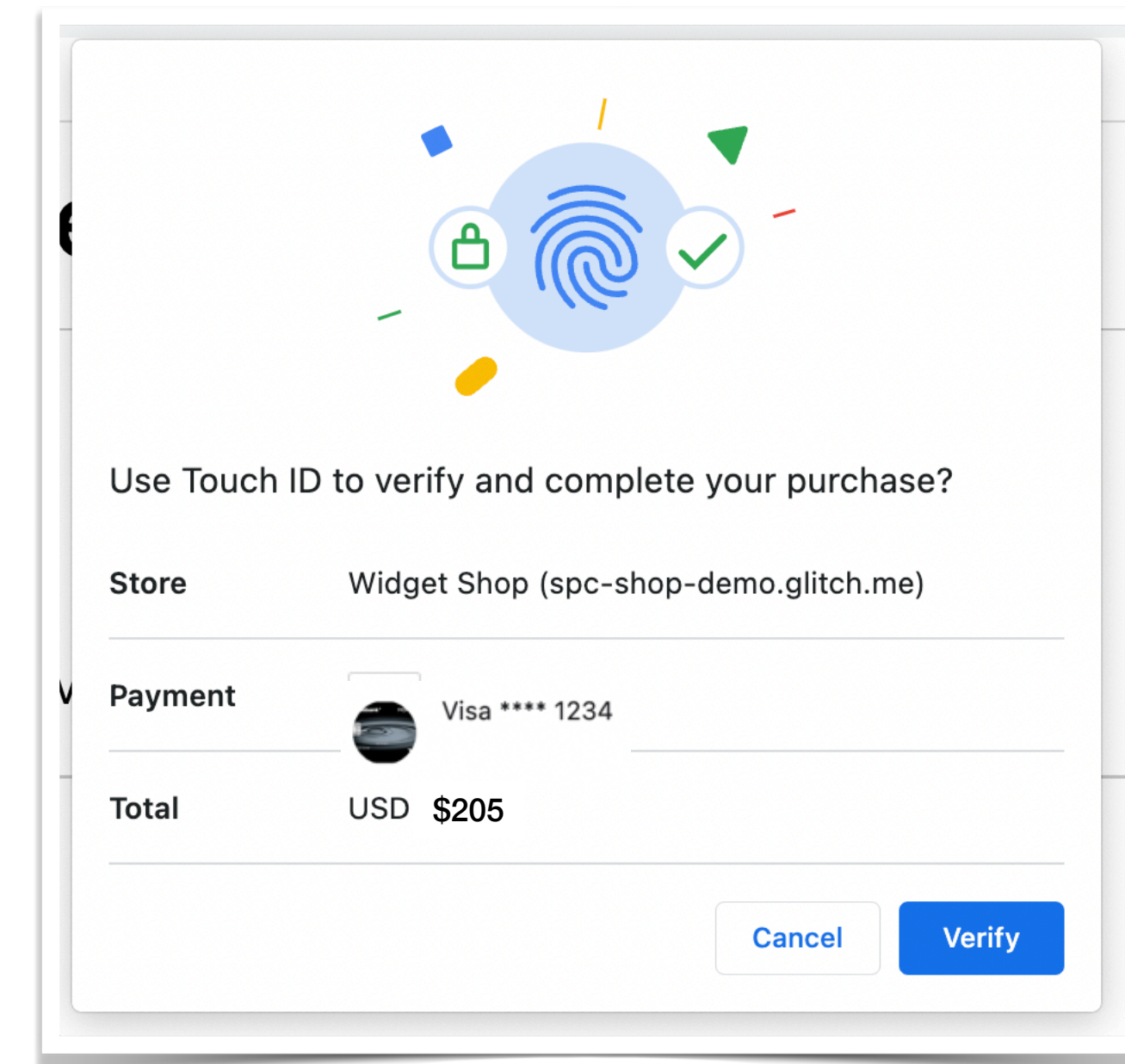
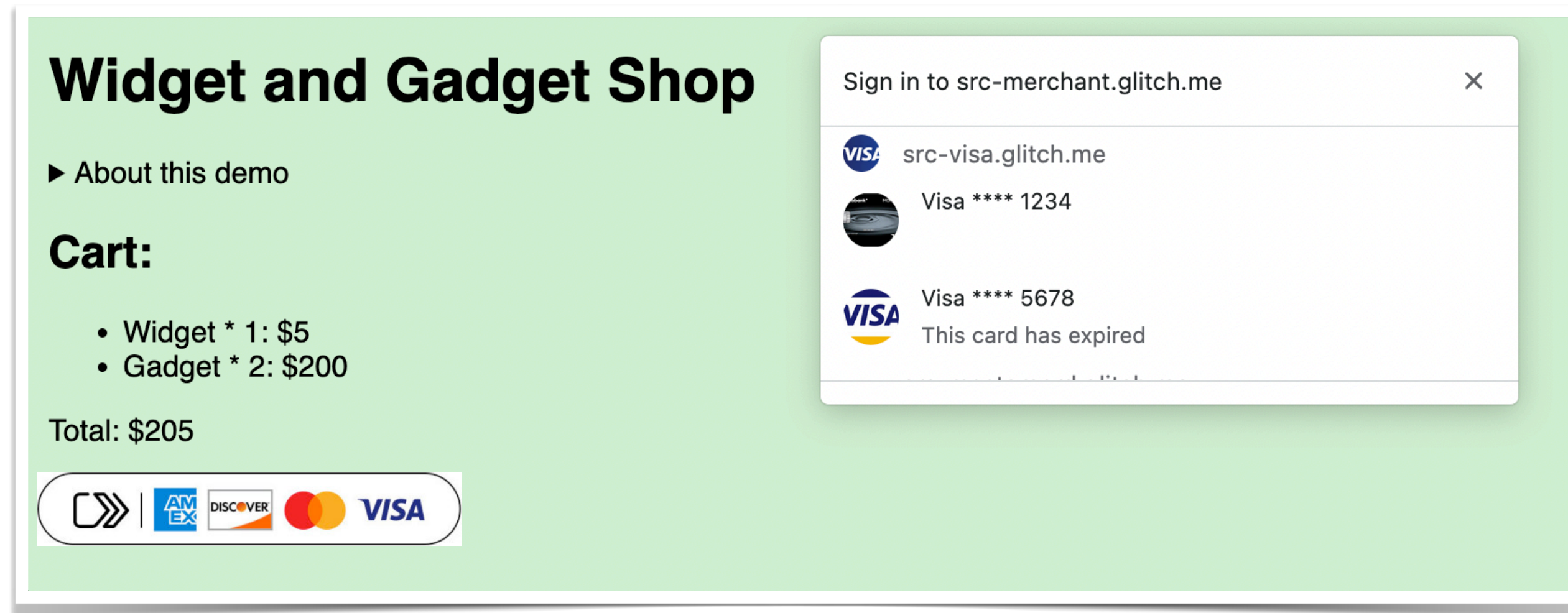
- * Privacy protecting federated login (FedCM)
- * Privacy protecting device recognition (Private State Tokens)
- * Better user experience when FIDO credentials available (Conditional UI)
- * Other Proposals in the Antifraud Community Group (e.g., safe list, suspicious location info, device integrity attestation)
- * Restore access to first party cookies with user consent (Storage Access)
- * Treat multiple origins as same first party (First Party Sets)
- * More reliable information about user's login status

Privacy Friendly Federated Login for User Recognition?

- * Web site providers browser a list of identity provider origins
- * Browser reaches out without saying what origin user is on
 - * Because no cross-origin exchange, IDPs are allowed to access 1p cookies and determine if user is logged in.
- * Where user is logged in, IDPs return account names
- * Browser displays them (without site awareness) for user selection
- * Only after selection do site and selected IDP know each other



Could we do EMV® SRC with these new features?



Upon click, get identity and card data from any SRC system where the user has authenticated. Before user action:

- SRC systems do not yet know which merchant
- Merchant does not know about identities/cards

Upon card selection, authenticate user with SPC

Note: This does not work today, but could with some implementation changes. [See Chrome FedCM demo.](#)

Coming Up

- * SPC to “Candidate Recommendation”; pilot results; more browser support
- * Develop next SPC use cases (e.g., recurring payments, non-payment applications)
- * Solidify SPC/FIDO alignment
- * Develop and incubate antifraud proposals

Other trends and relevant W3C work

Strong

Relevant

Tangential

Not yet



- ECommerce
- Digital Wallets
- Strong Customer Authentication
- Fraud mitigation
- Accessibility, Privacy, Security
- Digital Identity
- Real-time payments
- Deferred payments
- Micropayments / Buy-now-pay-later
- Cross-border payments
- Cryptocurrencies
- Central Bank Digital Currencies
- Contactless payments
- Peer-to-peer payments
- Metaverse
- Miniapps
- AI
- Financial Inclusion
- Sustainability

Thank you

* Check out WPSIG's [How EMVCo, FIDO, and W3C Technologies Relate](#)

* *We expect to publish updated version for 2022 in late November or early December.*

* *This version focuses on EMV® 3DS, FIDO, and SPC.*

* Get involved

* Anyone may join a Community Group at no cost

* FIDO Alliance and W3C Members may join the Web Payment Security Interest Group

* Contact me: ij@w3.org