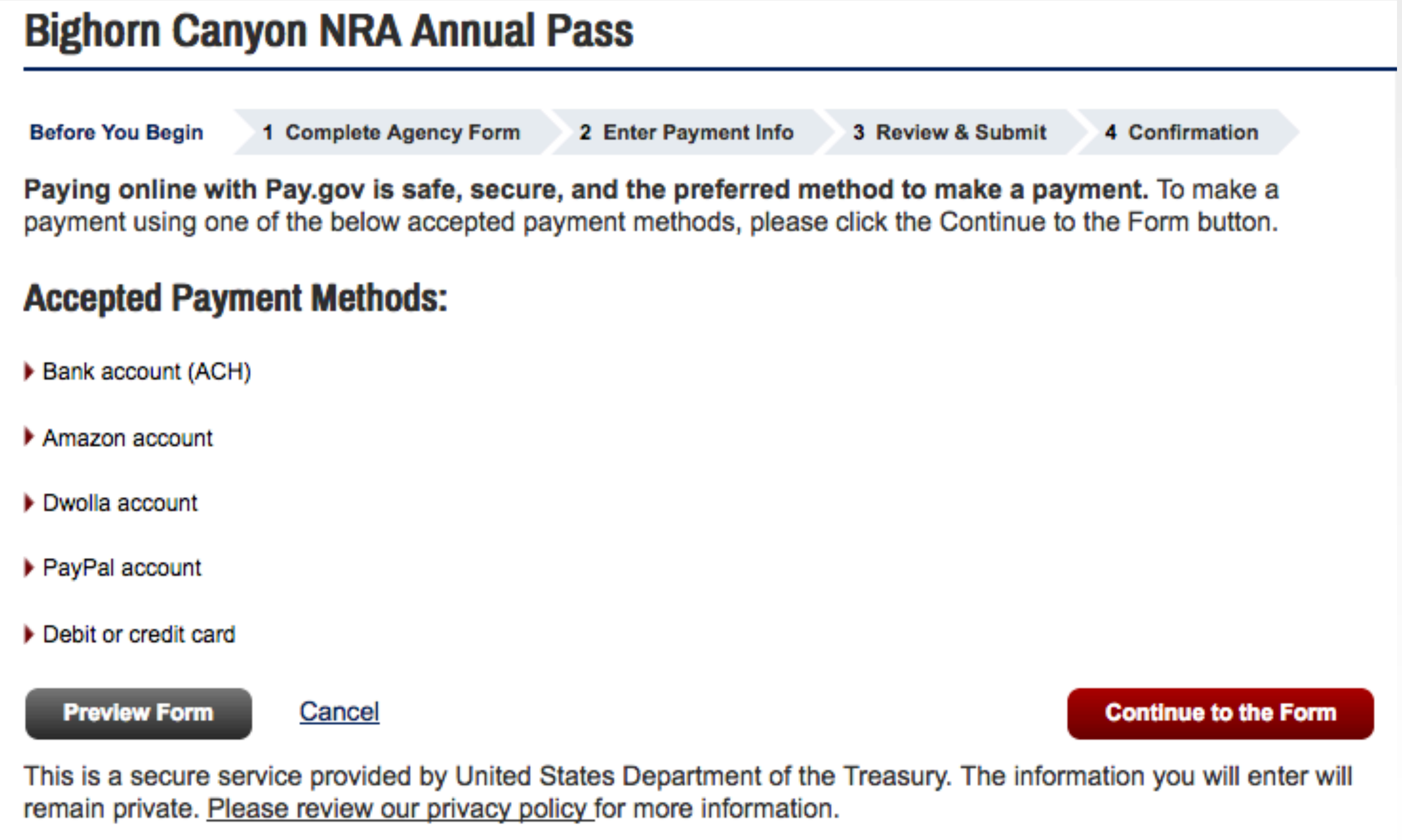
Improving Payments on the Web

Ian Jacobs
W3C

Making a Payment from pay.gov today

Step 1



Bighorn Canyon NRA Annual Pass

Paying online with Pay.gov is safe, secure, and the preferred method to make a payment. To make a payment using one of the below accepted payment methods, please click the Continue to the Form button.

Accepted Payment Methods:

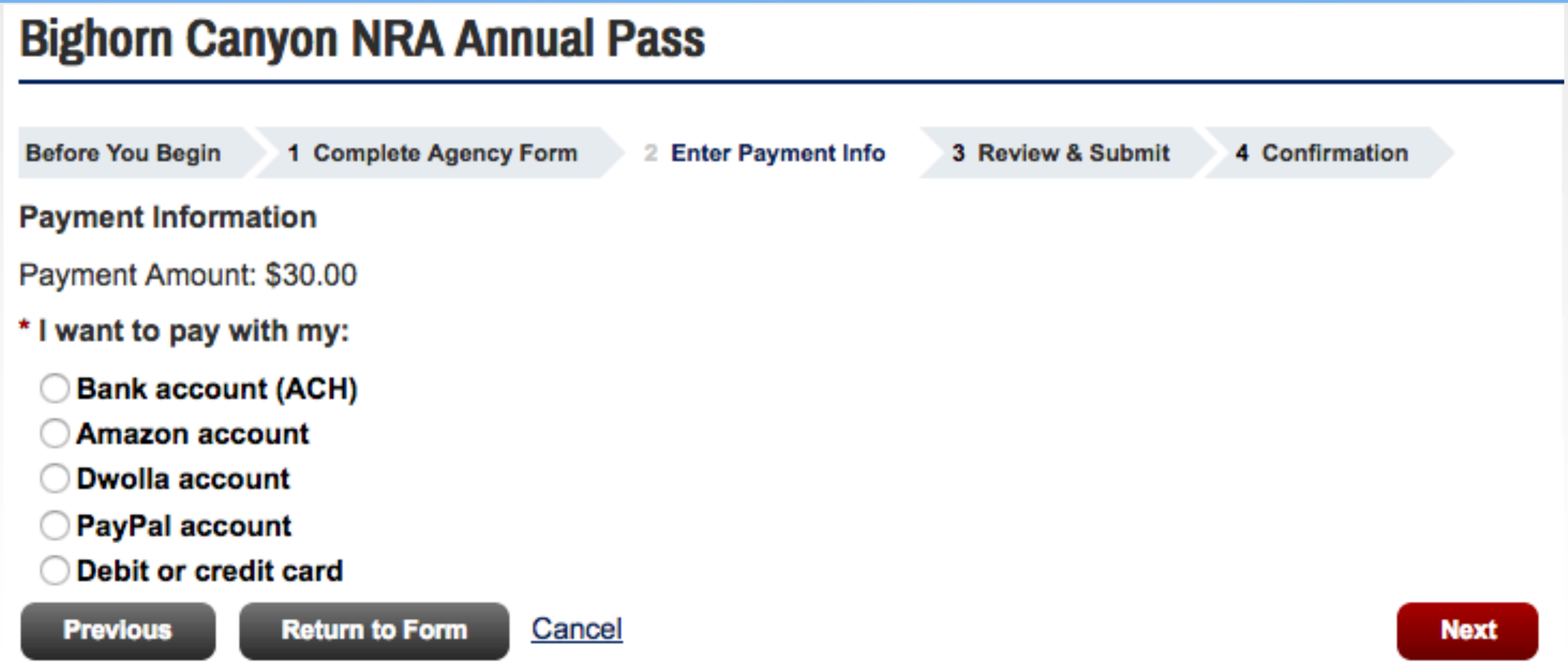
- Bank account (ACH)
- Amazon account
- Dwolla account
- PayPal account
- Debit or credit card

This is a secure service provided by United States Department of the Treasury. The information you will enter will remain private. Please review our privacy policy for more information.

Source: pay.gov

Selection of payment method

Step 2



Bighorn Canyon NRA Annual Pass

Payment Information

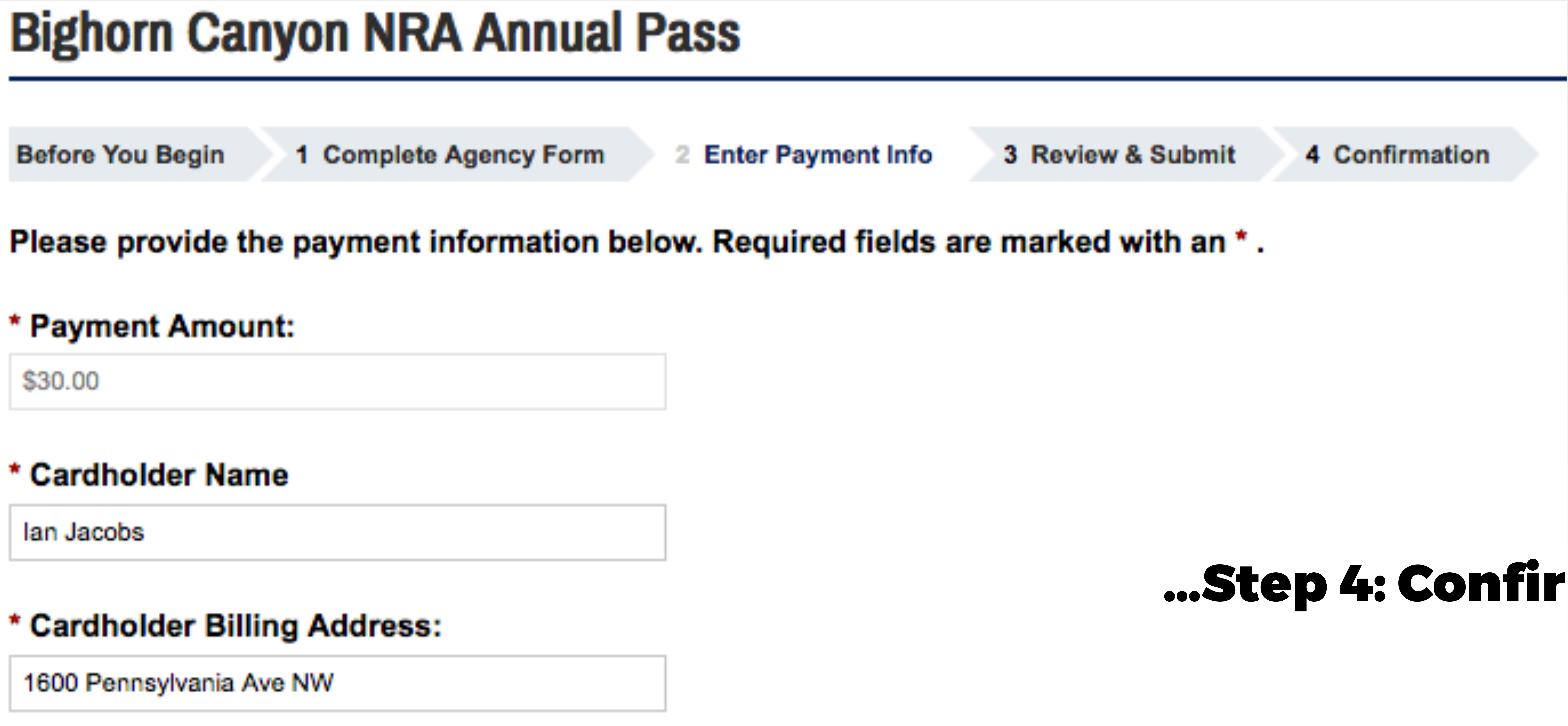
Payment Amount: $30.00

* **I want to pay with my:**

○ **Bank account (ACH)**
○ **Amazon account**
○ **Dwolla account**
○ **PayPal account**
○ **Debit or credit card**

Card Payment (all data not shown)

Step 3



Bighorn Canyon NRA Annual Pass

Please provide the payment information below. Required fields are marked with an * .

* Payment Amount:

$30.00

* Cardholder Name

Ian Jacobs

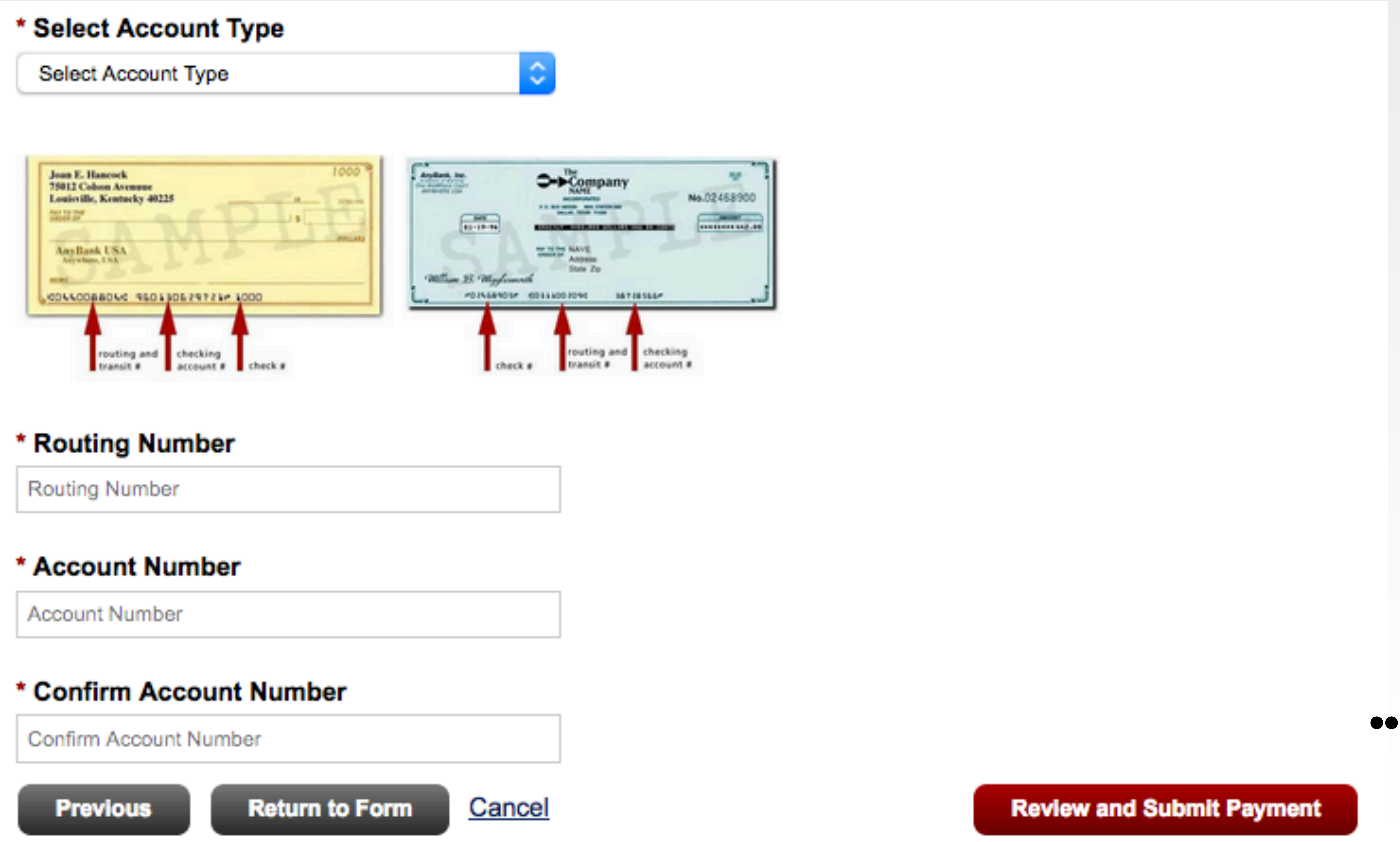
* Cardholder Billing Address:

1600 Pennsylvania Ave NW

…Step 4: Confirm…

ACH Payment (all data not shown)

Step 3 (Alt)



* Select Account Type

Select Account Type

* Routing Number

Routing Number

* Account Number

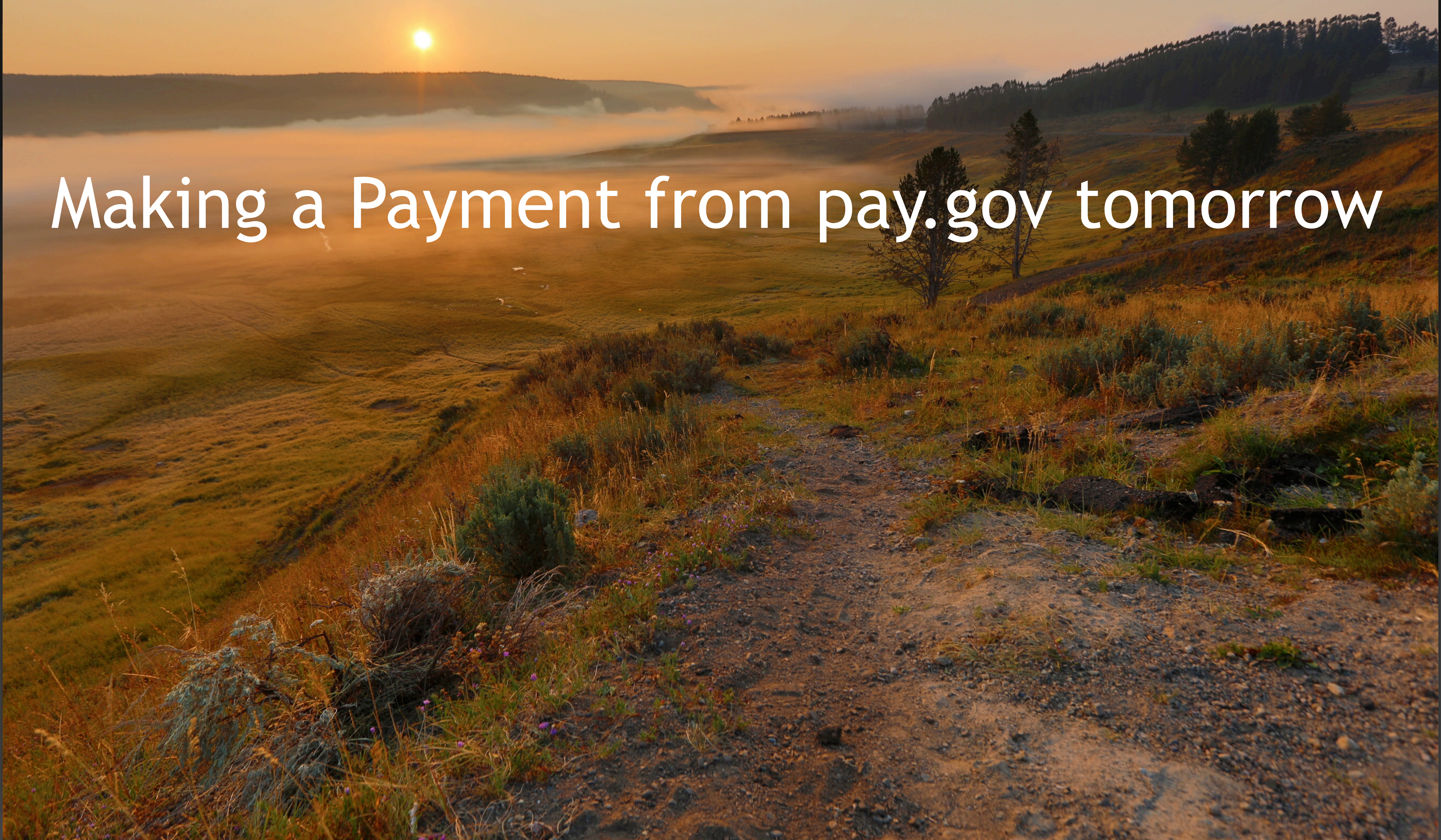
Account Number

* Confirm Account Number

Confirm Account Number

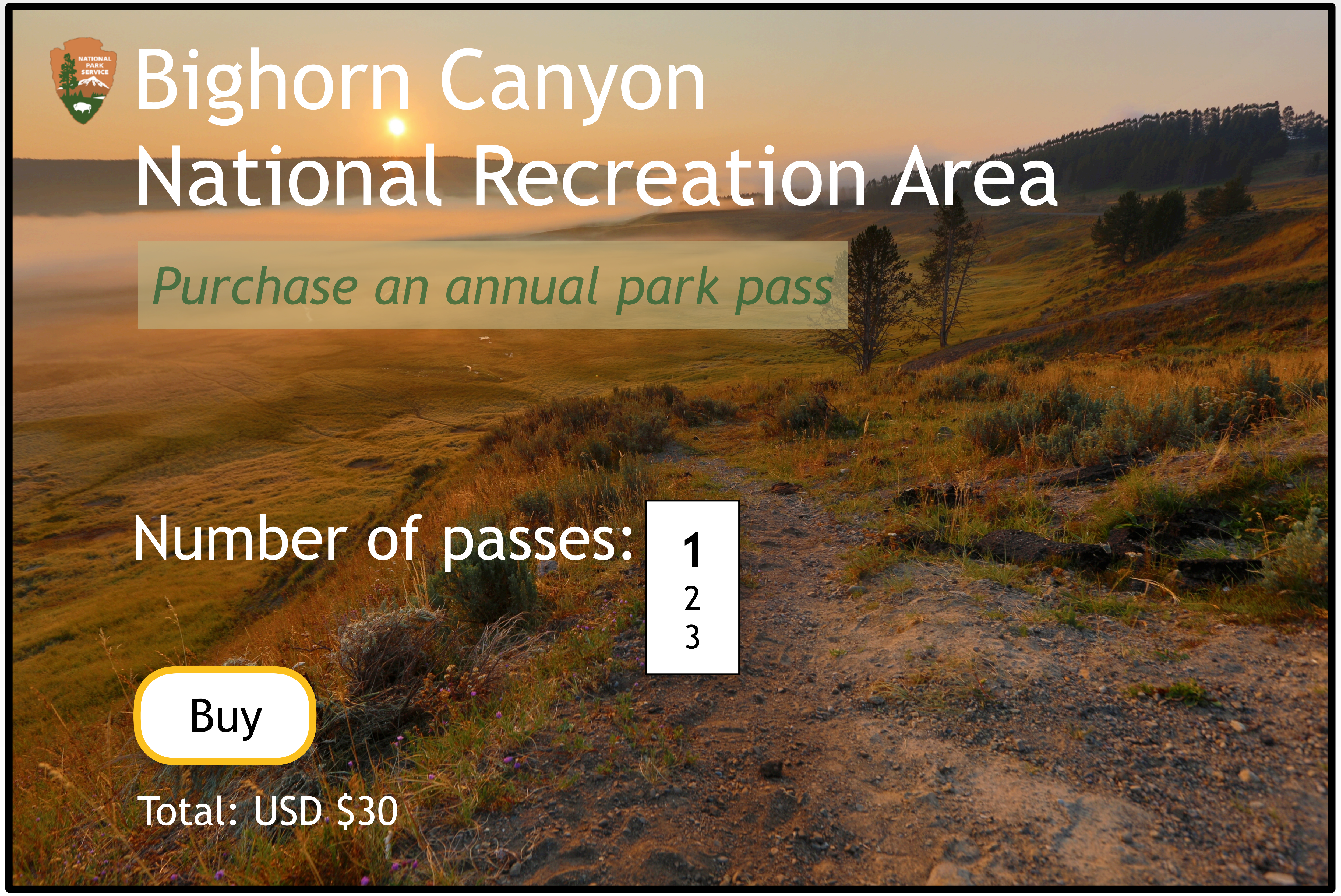
…Step 4: Confirm…

Making a Payment from pay.gov tomorrow



Choose the number of passes

Step 1



Bighorn Canyon
National Recreation Area

Purchase an annual park pass

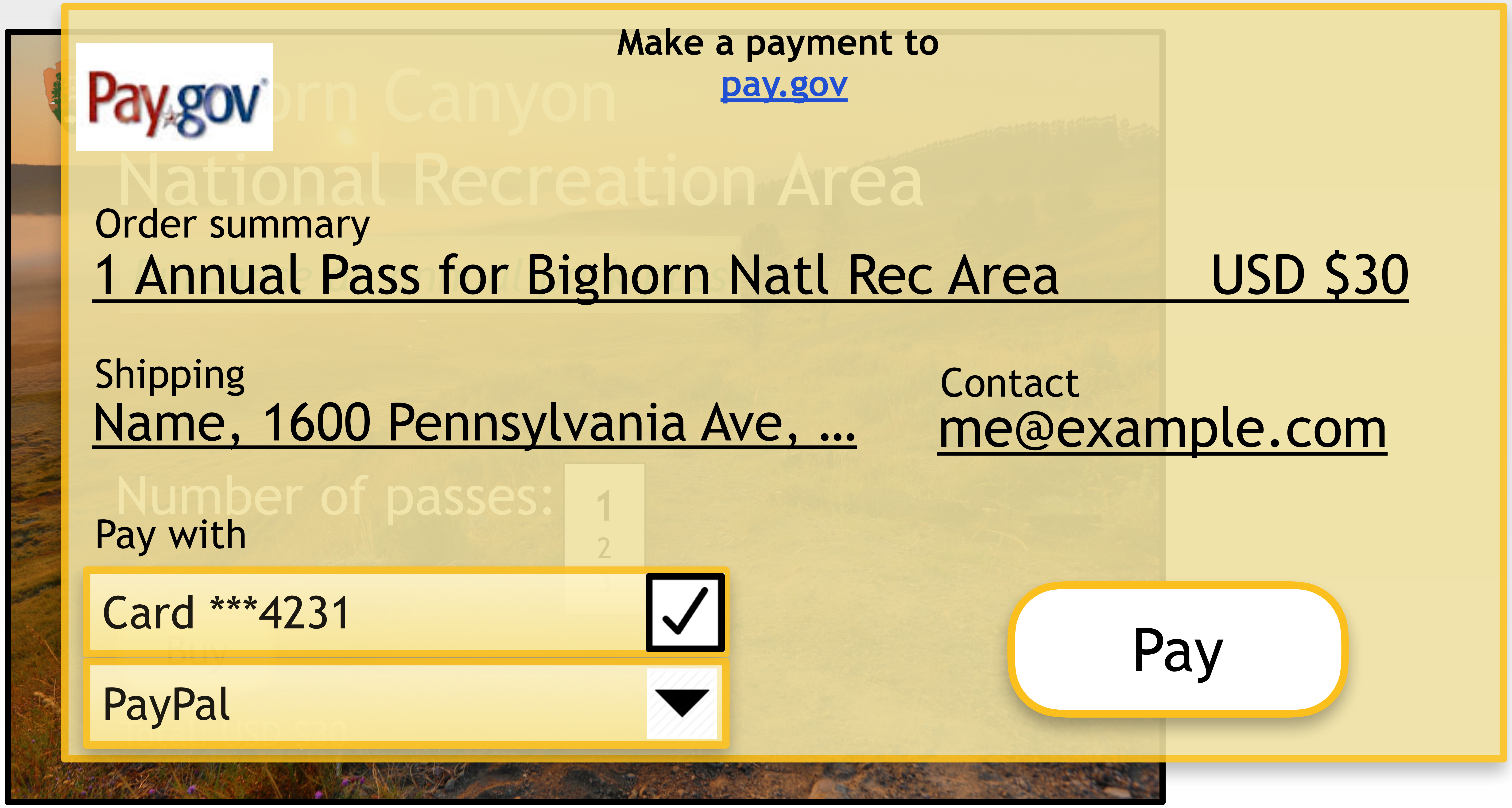
Number of passes: 1 2 3

Buy

Total: USD $30

Choose a payment app with stored creds

Step 2



Make a payment to
pay.gov

Order summary

1 Annual Pass for Bighorn Natl Rec Area USD $30

Shipping
Name, 1600 Pennsylvania Ave, …

Contact
me@example.com

Pay with

Card ***4231 ☑

PayPal ▼

Pay

How it Works

- Browser stores information useful at checkout
  - Name
  - Shipping Address
  - Contact information (email, phone)
  - Shipping type (e.g., delivery, pickup, none)
- Browser stores **basic card** information
- User registers **payment apps** with browser
  - Payment apps handle different **payment methods** (proprietary, card, ACH, etc.)

I. The Web Was Not Designed for Payments

Source: merchandisingmatters.com

Poor Experience Leads to Abandonment

- Usability challenges on mobile
  - Small screens, keyboards
- Mobile wallet fragmentation
- Complex check-out
- User payment preference not offered
- Different experiences on all sites
- Different experiences in-app, proximity, Web

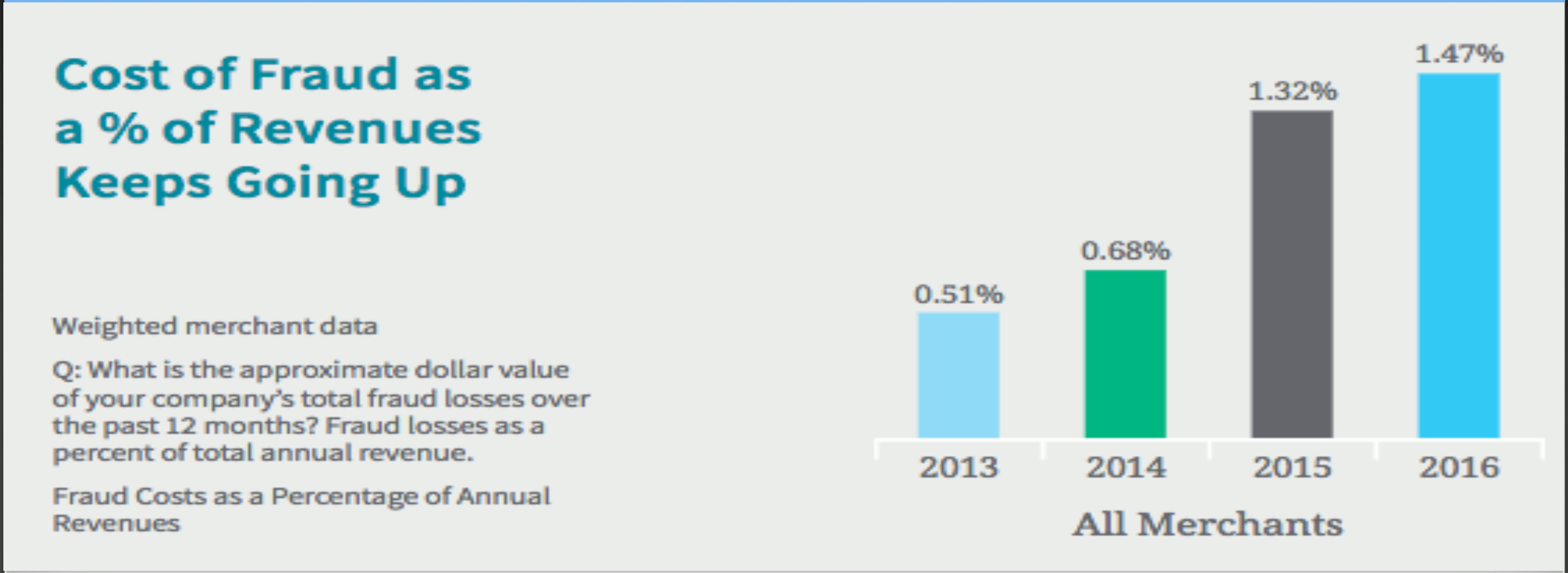
Source: Capital Numbers

Poor Security Leads to Lost Loyalty…

- Passwords are inadequate
  - Multi-factor authentication not well-integrated
- User interface complexity creates attack opportunities (e.g., phishing)
- Distributed applications create attack opportunities (e.g., cross-site scripting)
- Standard crypto primitives not available to Web applications

> *"After a security breach, 12% of loyal shoppers stop shopping at that retailer, and 35% shop at the retailer less frequently."*
>
> \- Forrester Research

…and Increased Costs



Cost of Fraud as a % of Revenues Keeps Going Up

Weighted merchant data

Q: What is the approximate dollar value of your company's total fraud losses over the past 12 months? Fraud losses as a percent of total annual revenue.

Fraud Costs as a Percentage of Annual Revenues

Source: Lexis Nexis

Web Scale Improvements Call For Standards

- Many standards bodies exist
  - ISO, EMV, PCI, X9, IEEE, NIST, …
- Interfaces between Web stack, applications, underlying payment systems not generally standardized
- Inadequate integration. Specifically, no standard APIs for wallet access, raising implementation costs for payment services providers; tokenization not part of the Web, biometrics not yet part of the Web

II. Who is W3C?

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

Key Facts

- Founded in 1994 by Web inventor Tim Berners-Lee
- ~425 Members; full-time staff ~75
- Community of thousands
- Liaisons to drive interoperability
  - ISO TC 68, ISO 20022, IETF, …
- Hundreds of specifications (royalty-free)

W3C is Building an Open Web Platform

- The Open Web Platform is a full-fledged programming environment for rich, interactive, cross-platform applications
- HTML5 is the cornerstone
- Most interoperable platform in history
- A billion Web sites
- Millions of developers

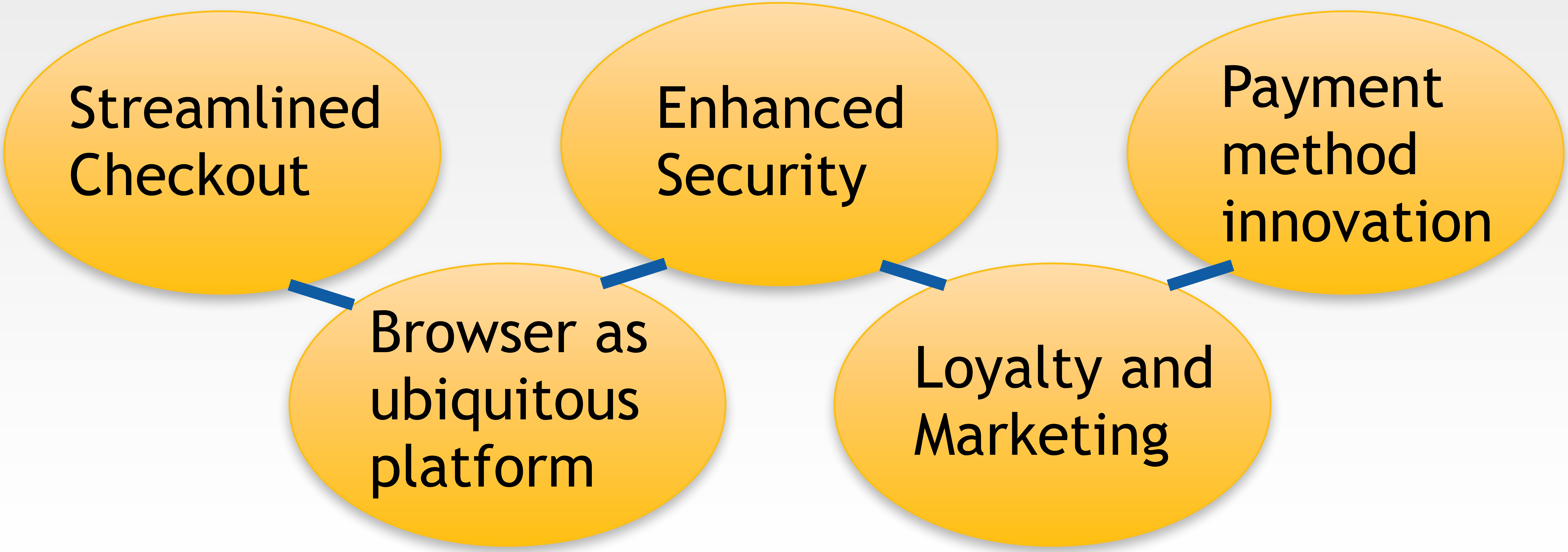
Including Built-In Payments Capabilities

“We are long overdue for a payments user interface for the web.”

-- Tim Berners-Lee

[What if ‘One Click’ Buying Were Internetwide?](#)
New York Times, 25 September 2016

III. The Road to More Web-Like E-Commerce



Streamlined Checkout

Enhanced Security

Payment method innovation

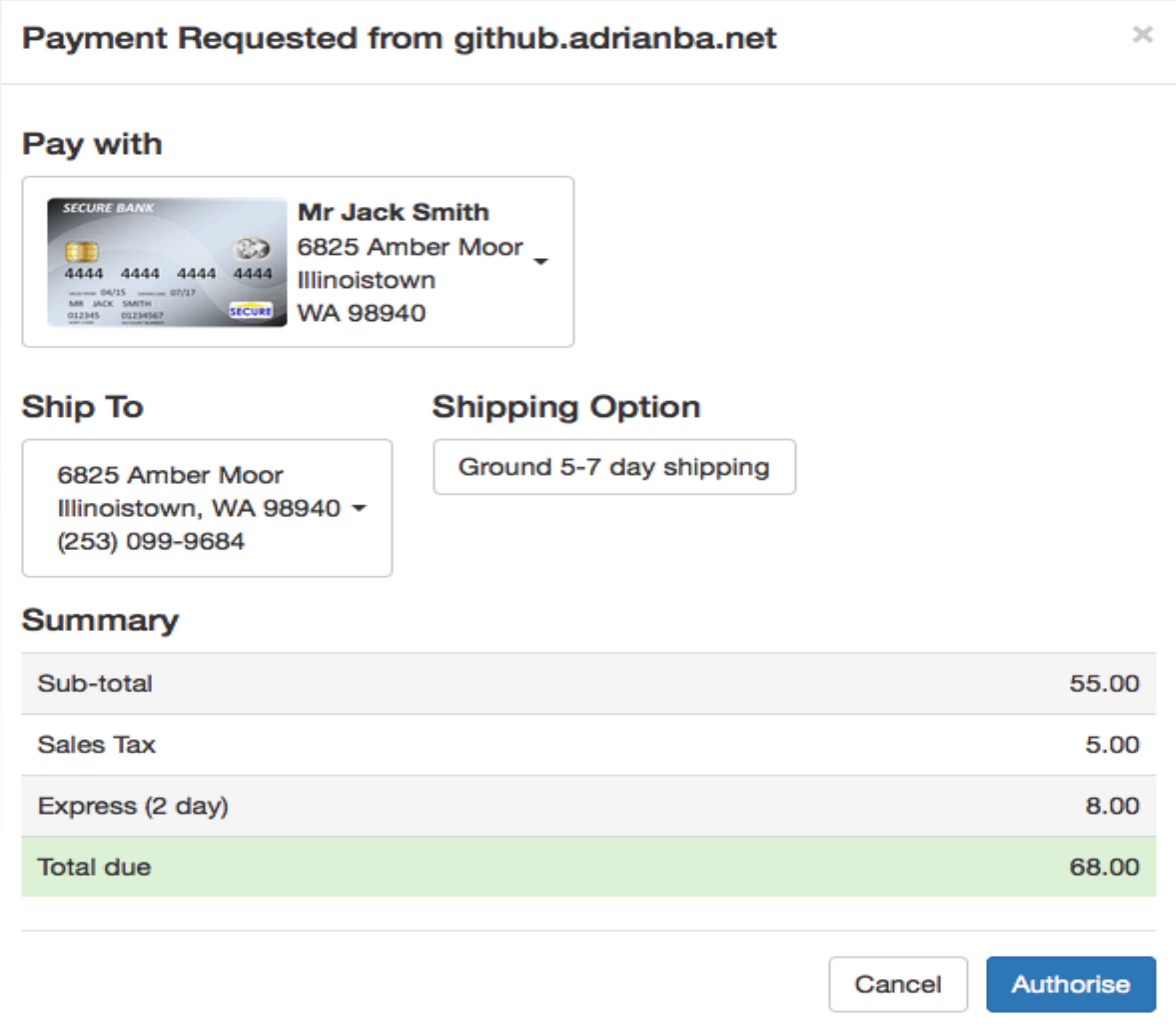
Browser as ubiquitous platform

Loyalty and Marketing

Streamlined Checkout

Source: surfingaustralia.com

Demo



Payment Requested from github.adrianba.net

Pay with

Mr Jack Smith
6825 Amber Moor
Illinoistown
WA 98940

Ship To

6825 Amber Moor
Illinoistown, WA 98940
(253) 099-9684

Shipping Option

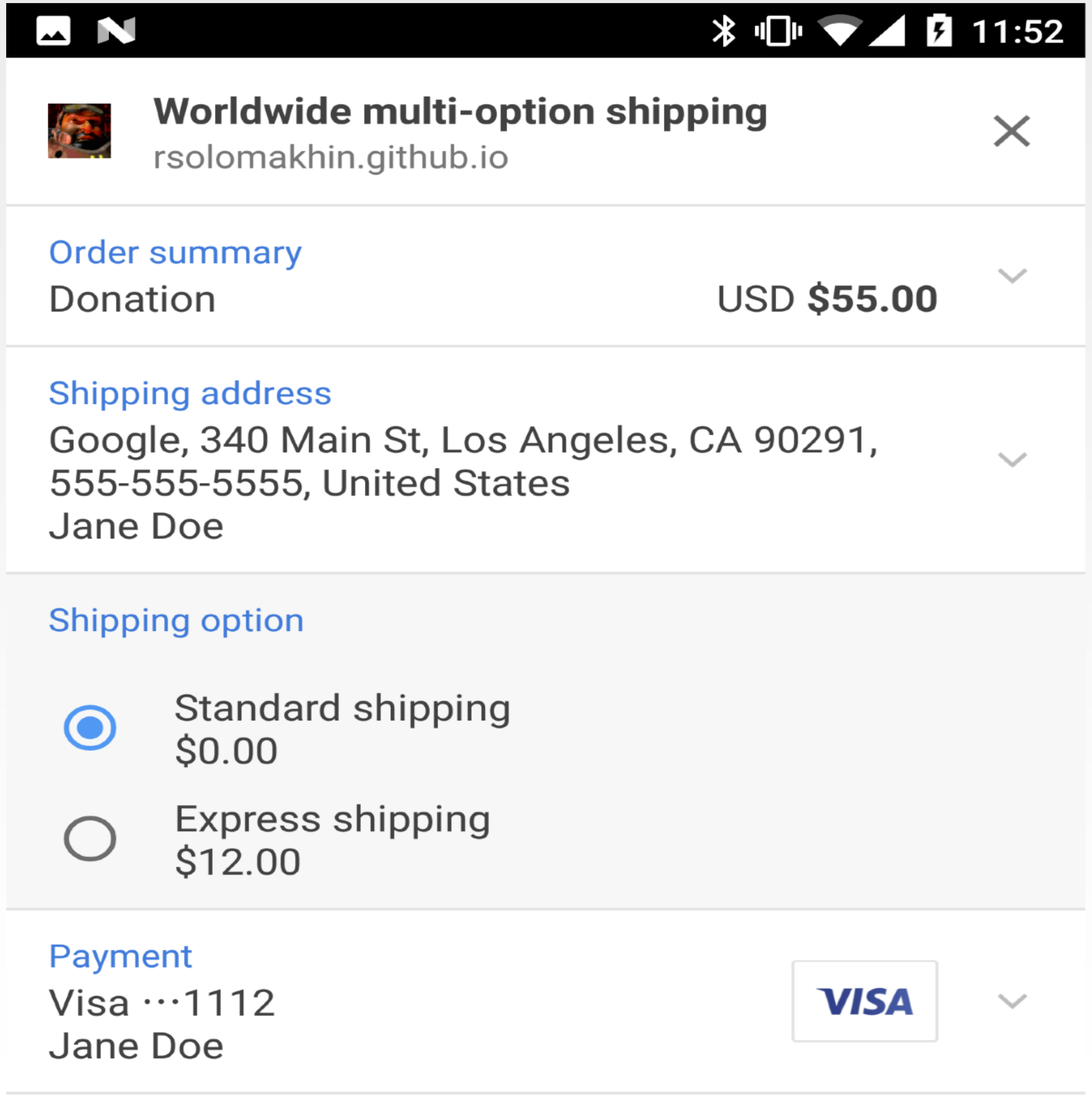
Ground 5-7 day shipping

Summary

Sub-total	55.00
Sales Tax	5.00
Express (2 day)	8.00
Total due	68.00

- Demo by Adrian Bateman (Microsoft)

Chrome/Android Beta Available



Worldwide multi-option shipping
rsolomakhin.github.io

Order summary
Donation USD **$55.00**

Shipping address
Google, 340 Main St, Los Angeles, CA 90291,
555-555-5555, United States
Jane Doe

Shipping option

● Standard shipping
$0.00

○ Express shipping
$12.00

Payment
Visa ···1112
Jane Doe

- “Payment Request API Guide” (Google)

Key Ideas for “Payment Request API”

- Replace forms with native browser UI for payment info (card, address, etc.)
  - Browser chrome is fast
  - Improves security -- harder to spoof than Web page
- Simplify user experience (UX), especially on mobile
  - User reuses data without re-typing
  - Browser only shows matching payment methods, so less noise
  - User can find preferred payment method without scanning page
  - Browsers distinguish themselves through optimized UX (e.g., 1-click)

Please Note

- Neither Payment Request API nor browser submits payment for processing
  - Data returned by API depends on payment method (e.g., PAN, EMV token)
- Goal of API is to facilitate information collection and return to merchant
  - Merchant (or gateway) still needs to handle data they receive
- Authentication is handled by another W3C group
  - Web Authentication Working Group

Open Ecosystem of 3rd Party Payment Apps

- Payment Request API only supports browser-stored card credentials

- A complementary API will enable third party payment apps
  - User registers payment apps from many sources: banks, merchants, mobile operators, etc.
  - Merchant may recommend payment apps during checkout
    - *Note this is a new way for users to learn about and register (payment) apps*
  - Payment apps support different payment methods (e.g., cards, credit transfers, proprietary methods, distributed ledgers, etc.)

- Payment apps will distinguish themselves through services
  - Usability, strong authentication, tokenization, location services, loyalty programs, etc.

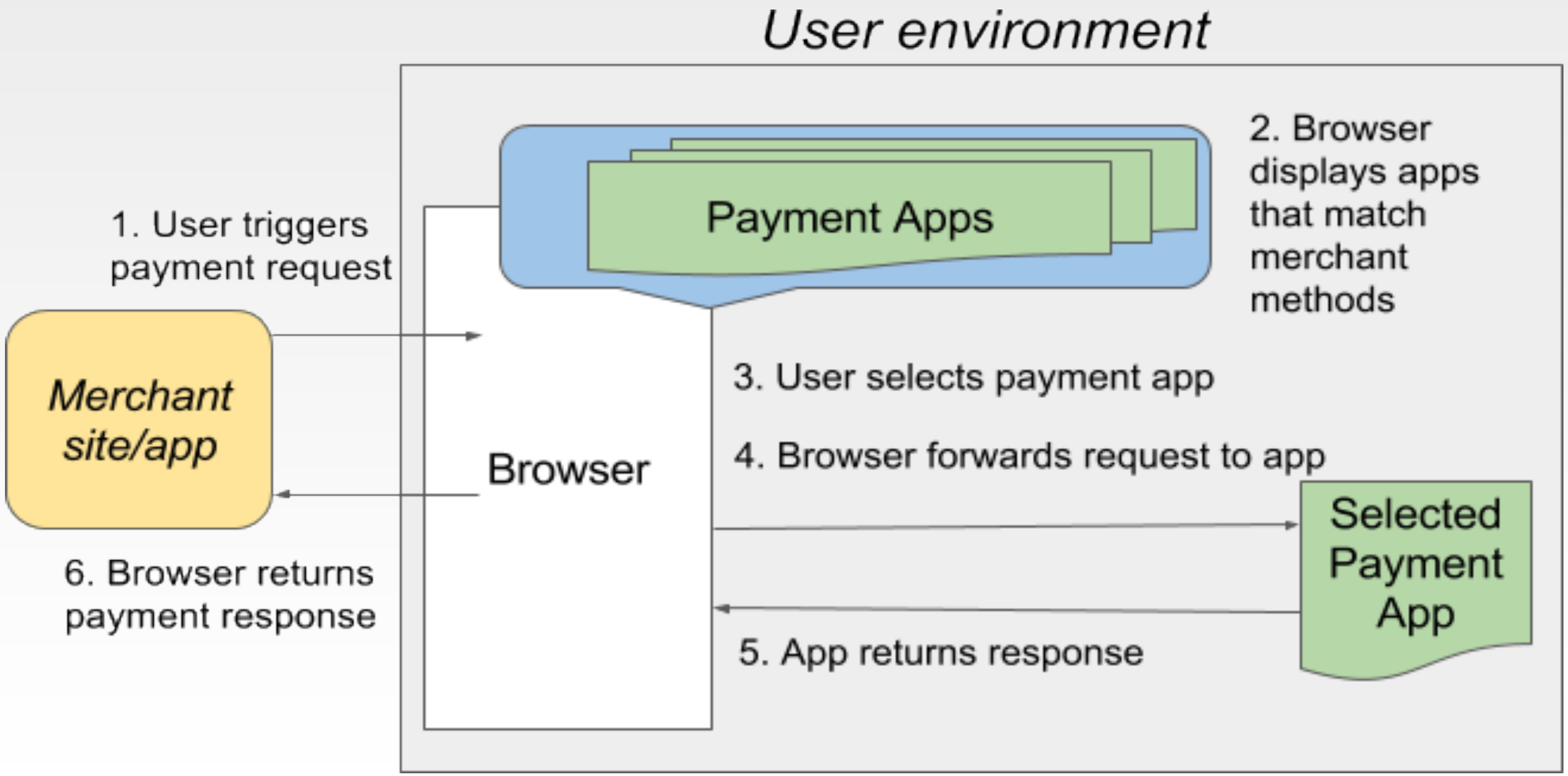
Merchant Perspective

- Consistent, simpler UX should increase conversions
- Enables a branded, harmonized experience across channels through (retailer) payment apps
- Merchant payment apps can integrate loyalty and points
- Facilitates adoption of payment method improvements (e.g., to improve security)
- Increased support for user preferred payment methods

Payment Gateway Perspective

- Cross-device interoperability at lower cost (benefit of using the Web)
- Lower cost to build checkout
- Can support more payment methods without more complex UX
  - Thanks to browser “match making”

Flow



User environment

1. User triggers payment request

Merchant site/app

Browser

Payment Apps

2. Browser displays apps that match merchant methods

3. User selects payment app

4. Browser forwards request to app

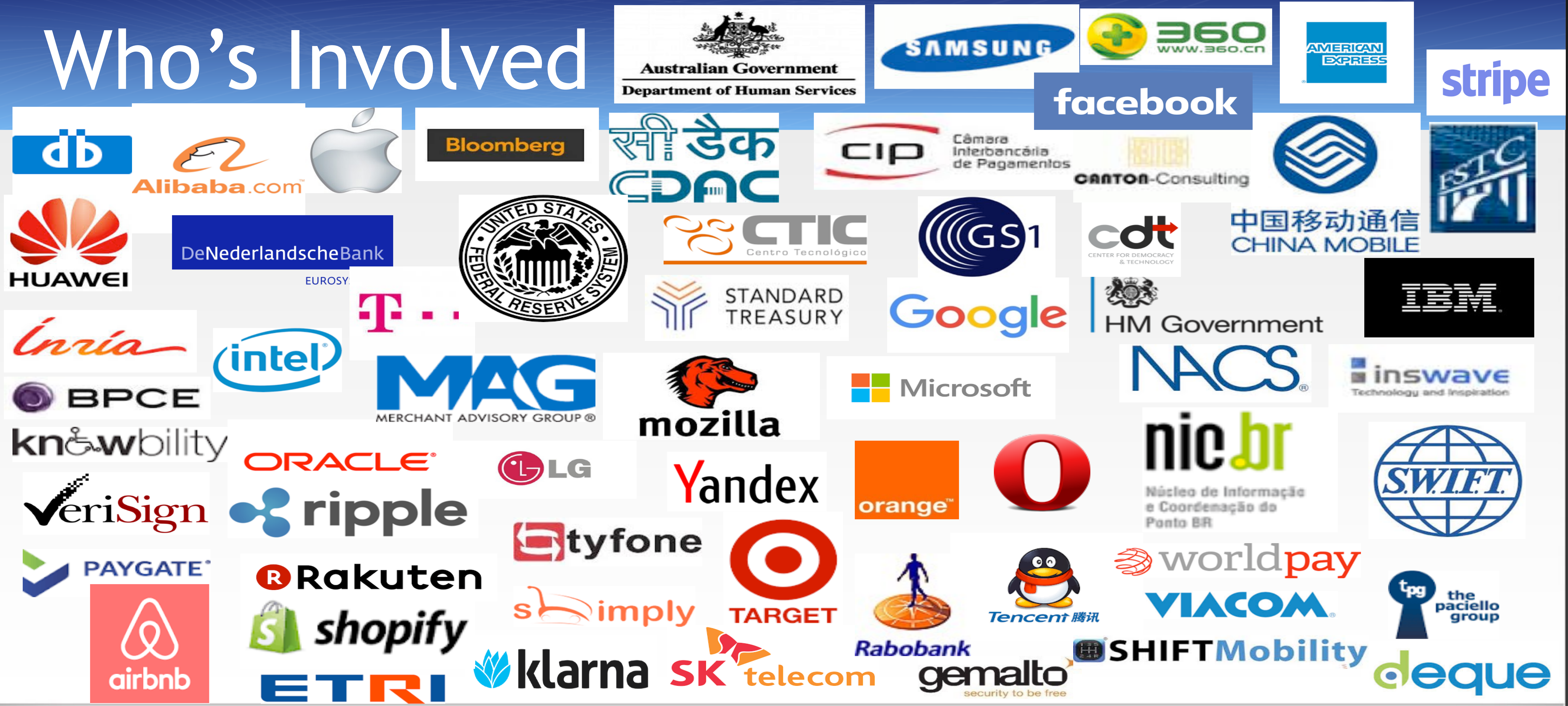
Selected Payment App

5. App returns response

6. Browser returns payment response

W3C®

Who's Involved



Status

- Implementing: Google, Microsoft, Facebook, Samsung, Mozilla, Opera
- Works started on payment app integration: Alipay, Samsung, Google, Amex, Facebook, Worldpay, Stripe, Klarna, Gemalto, …
- Apple announced “Apple Pay on the Web” and stated goal within Web Payments Working Group of convergence to a “solid, cross-browser framework for payments.”
- Gathering feedback from experiments with merchants, E-Commerce providers, proprietary payment app providers

Enhanced Security

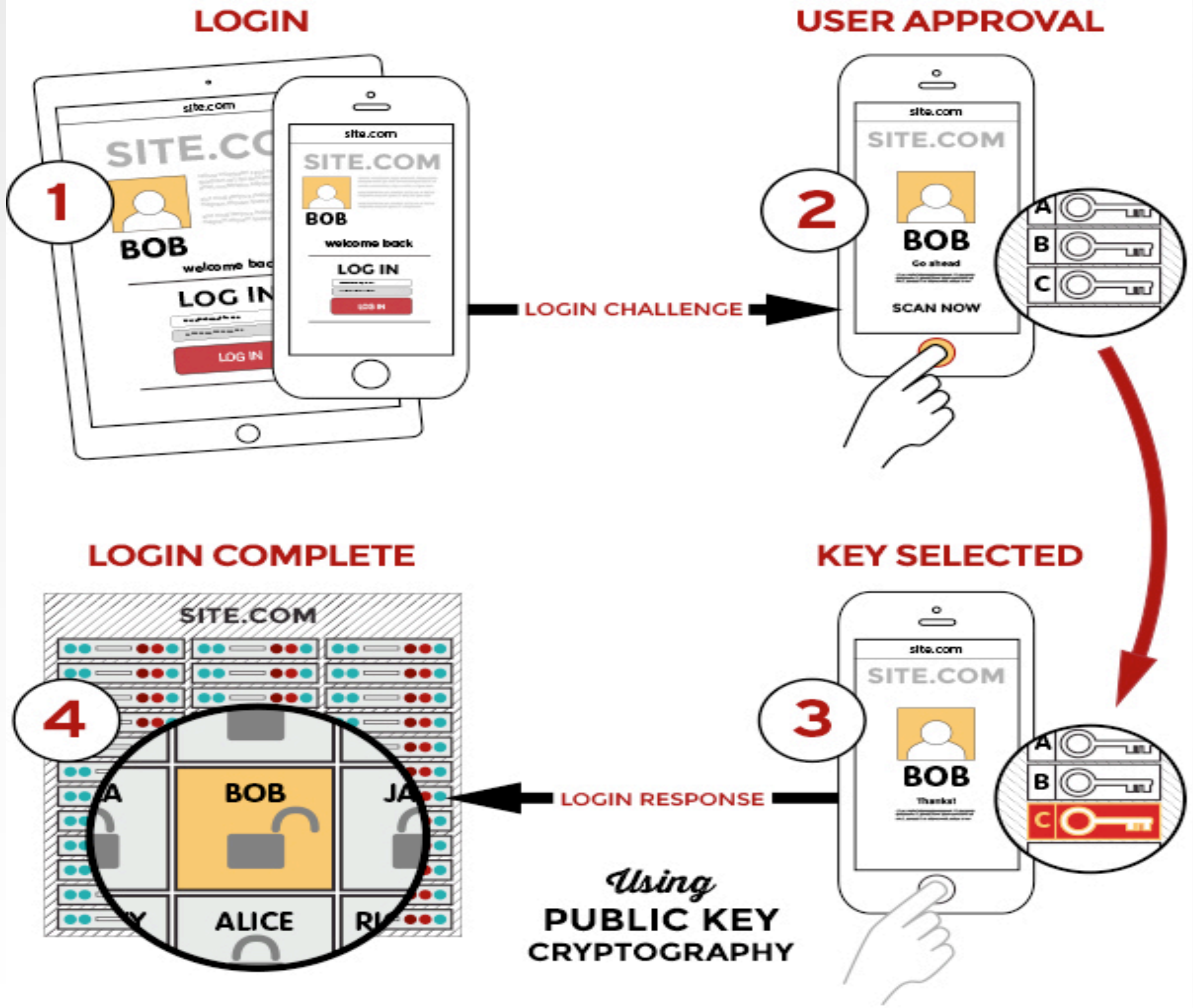
Source: skysports.com

Data Protection

- Crypto primitives for Web apps:
  - Hashing, signature generation and verification, and encryption and decryption, key management.
  - Widely supported in browsers; gaining broad interoperability.
- For:
  - Secure messaging
  - Multi-factor authentication
  - Protected document exchange
  - Cloud storage
  - Document signing
  - Data integrity

Strong Authentication

- Passwords weak
  - Phishing, data loss, liability
- Replace them with logins via USB key or smartphone.
- Collaboration with FIDO Alliance, who brought 2.0 specs to W3C
- [Launched 17 Feb 2016]()
- [First Working Draft published in May]()



Source: [fidoalliance.org]()

Application and Communication

- Protect apps against injection of unwanted or malicious code
- Assure the integrity, authenticity, and confidentiality of Web interactions
- Includes:
  - Secure communication channels
  - Apps delivered without spoofing, injection, eavesdropping
- Numerous specifications at different maturity levels, such as
  - Cross-Origin Resource Sharing, Content Security Policy, Subresource Integrity, Credential Management, …

Hardware Security

Incubation Phase

- Access to secure element and other hardware from apps
  - More general than Strong Authentication work
- Identity use cases (e.g., government issued identifiers) raise interesting privacy issues.
- Hardware Based Secure Services Community Group now:
  - Clarifying use cases
  - Documenting technical requirements
  - Planning to write draft API
  - Then will propose clearer charter

Source: Merchant Advisory Group

Verifiable Claims

Chartering Phase

- Problem statement from Credentials Community Group:

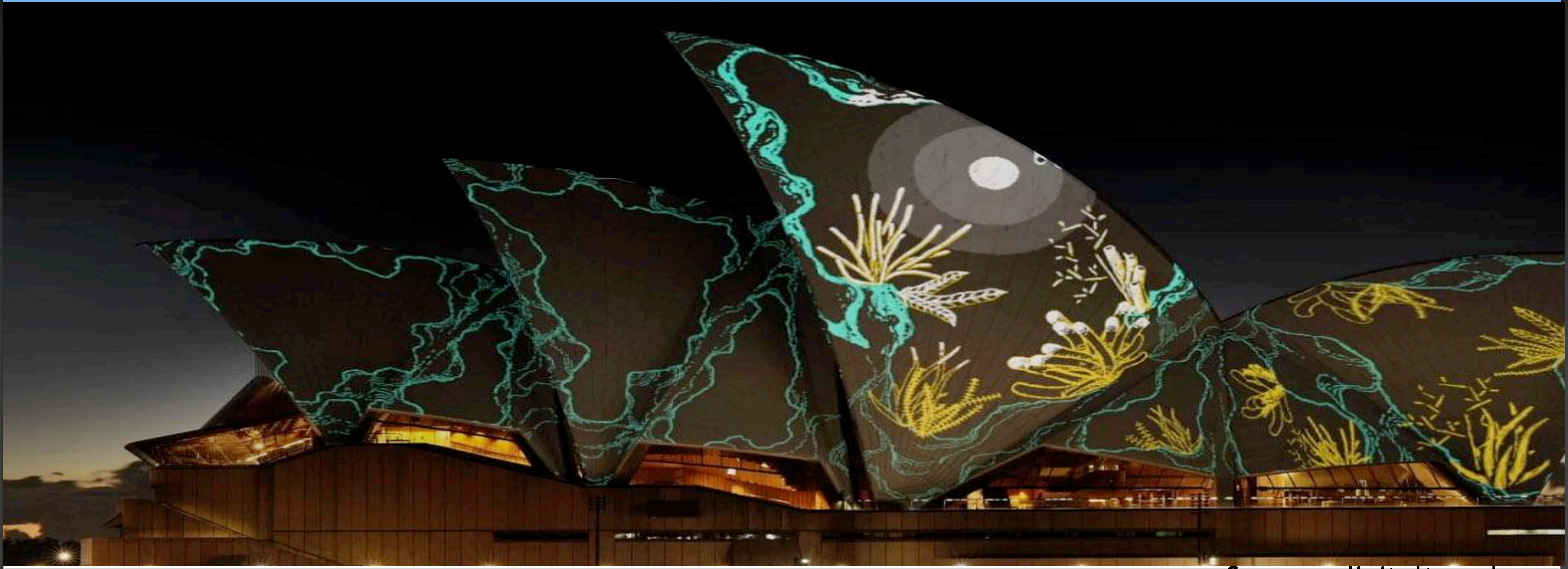
  "There is currently no widely used self-sovereign and privacy-enhancing standard for expressing and transacting verifiable claims (aka: credentials, attestations) via the Web."

- CG wrote use cases for several industries. Includes for financial services:
  - Lowering KYC costs
  - Money transfer
  - Setting up bank account from home

- Membership has reviewed a draft charter for a Verifiable Claims WG

  - W3C staff working with reviewers to resolve objections and increase consensus

Payment Method Innovation



Source: digitaltrends.com

Interledger Payments (ILP)

Incubation Phase

- Ripple brought to W3C (see white paper)
- Moving money between payment systems is costly and cumbersome
  - Users want payments to be simple, whatever the underlying systems
- Interledger bridges payment systems
  - Very Web-like vision
  - Anyone with accounts on two ledgers can connect them (and charge a fee)
  - Protocol ensures everyone paid, or no one
- ILP Community Group developing plan for specifications
  - Some specs likely to advance to a W3C Working Group

Loyalty and Marketing

Source: Renee Schmeider

Digital Offers

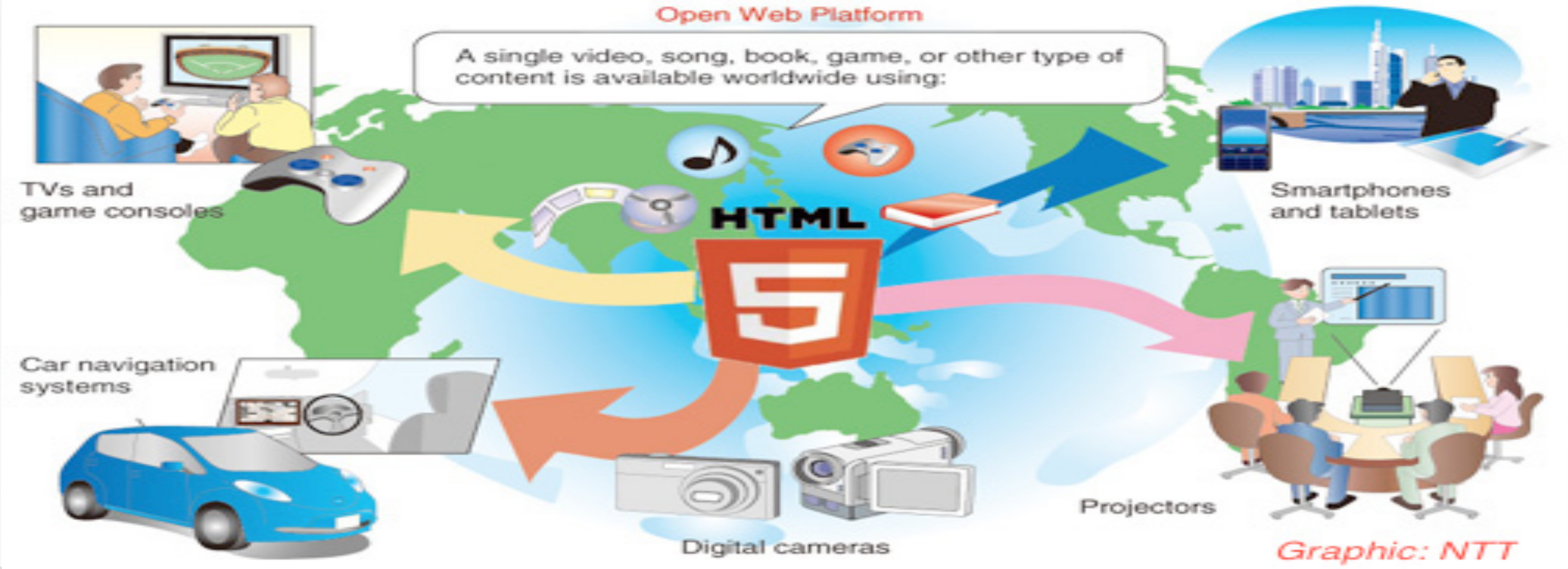
Incubation Phase

- Merchants interested in:
  - Coupons, loyalty, discounts, multi-tender
  - Harmonized experiences in-store and online
  - Omni-channel customer relations
- Coupons natural extension to Web payments API
  - Improve the Web for digital offers, including loyalty, coupons, rewards, points, and vouchers.
- Digital Offers Community Group
  - Launched **10 October** to develop gap analysis, use cases, incubate

“65% of customers use their smartphones to find coupons online… Retailers that can create experiences that serve consumers in context will drive both customer loyalty and business results.”

- Forrester Research

Browser as Ubiquitous Platform



Graphic: NTT

Broad Set of Activities to Enhance Browser

- Geolocation Working Group
  - Geolocation and geofencing
- Web Real-Time Comms WG
  - Real-time video/audio in the browser for remote enrollment?
- Paid Content CG
  - Discovery, pricing, transactions, storage
- Web Applications Working Group
  - Push notifications
- Web Bluetooth CG and Web NFC CG
  - Web app support for proximity payments?
- Blockchain CG

Help W3C Build the Web

Tim Berners-Lee featured at London Olympics 2012

Source: Guardian

Related US Treasury Objectives

- 1.4 Facilitate commerce by providing trusted and secure U.S. currency, products, and services for use by the public
- 3.2 Improve the disbursement and collection of federal funds and reduce improper payments made by the U.S. government
- 4.3 Improve the cybersecurity of our nation’s financial sector
- 4.4 Protect the integrity of the financial system by implementing, promoting, and enforcing anti-money laundering and counterterrorism financing standards

Source: Department of the Treasury Strategic Plan FY 2014-2017

Resources

- These slides: https://www.w3.org/2017/Talks/ij_payments_201701/w3c.pptx

- Contact: Ian Jacobs <ij@w3.org>

- More about W3C Payments https://www.w3.org/Payments/