

**stripe**

W3C Web Payments Working Group

# Secure Payment Confirmation Pilot

**March 2020**

btidor@stripe.com  
danyao@chromium.org  
adrian@coil.com

# Background

## Context

Focused on **payment authentication**, separate from credential entry (at least initially)

Compatible with existing payment authentication solutions, e.g. **3D Secure**

Payment context established by the **Payment Request API**

Users verified with **FIDO biometric authentication**

## Goals

Provide a **reliable, low-friction authentication mechanism** for users, merchants and banks

**Increase user confidence** with biometric confirmation of transaction details in browser-native UI

**Protect user privacy** by requiring explicit consent before confirming identity

**Stop phishing** + satisfy EU SCA requirements for **dynamic linking** by capturing transaction details in a tamper-proof cryptographic signature

*When used with 3D Secure...*

**Improve reliability** and solve Content Security Policy problems by avoiding the need to redirect to the issuing bank

**Gracefully degrade** to vanilla 3D Secure for unenrolled users and on unsupported devices

# Background

## API “Superpowers”

Browser **binds payment details** into cryptographic signature


Any merchant can request a signature from the issuer’s public key: **cross-origin credential sharing**

About the Secure Payment Confirmation API

# Enrollment Flow Mocks

Merchant checkout x +

merchant.com/cart



 T-shirt (Blue / M)  
**€2.00**

Powered by **stripe** | [Terms](#) [Privacy](#)

### Pay with card


Email

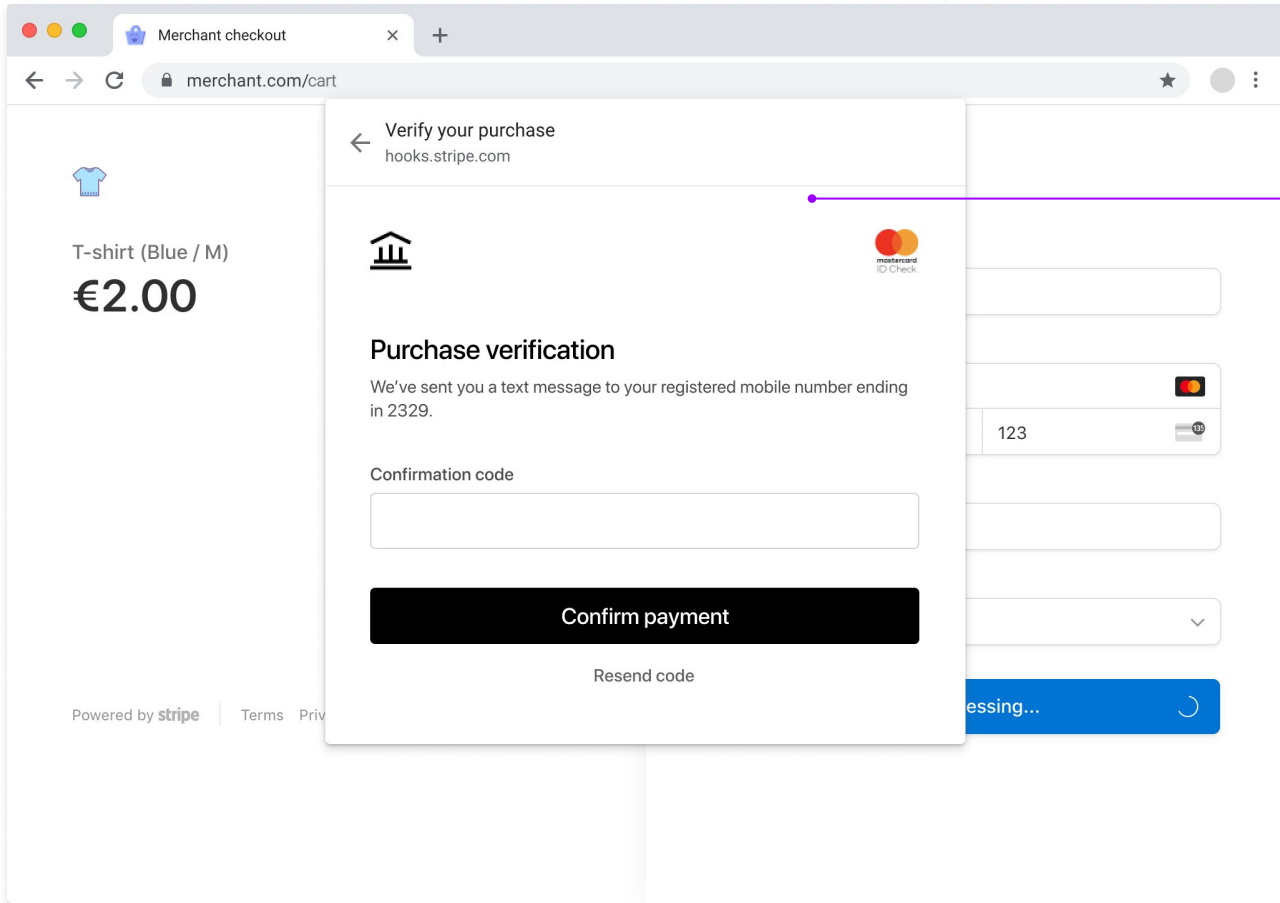
Card information

<input type="text" value="5555 5555 5555 4444"/>		
<input type="text" value="01 / 25"/>	<input type="text" value="123"/>	

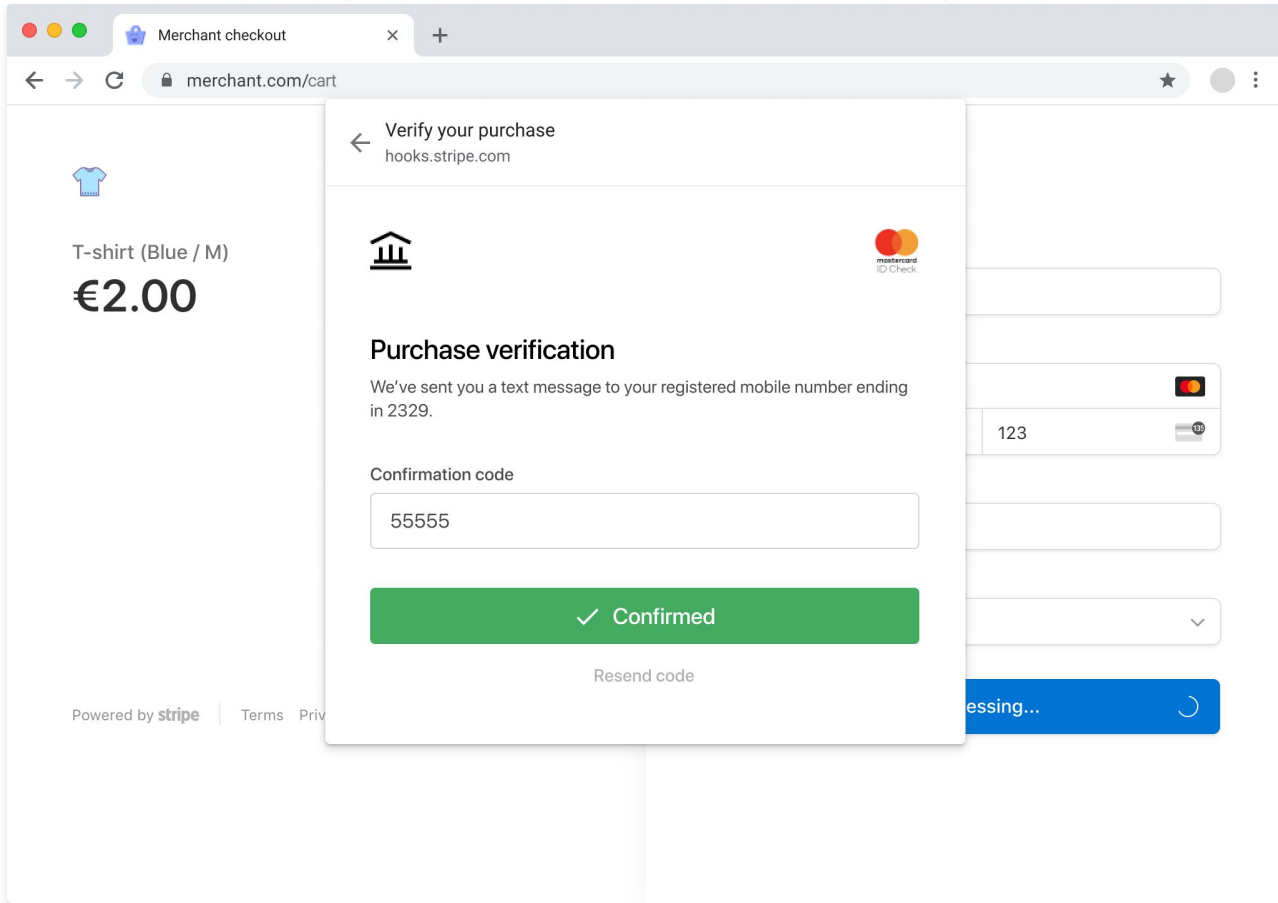
Name on card

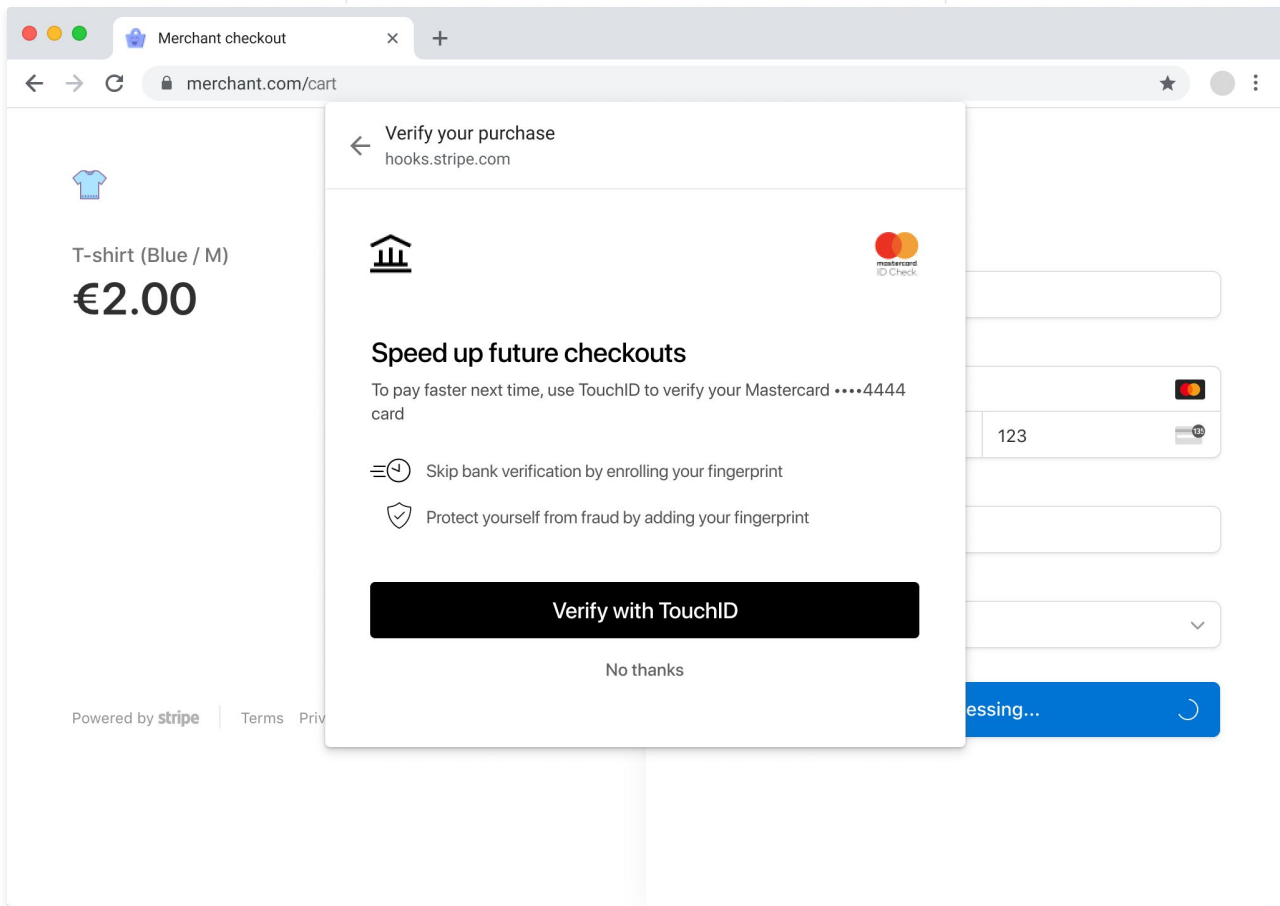
Country or region



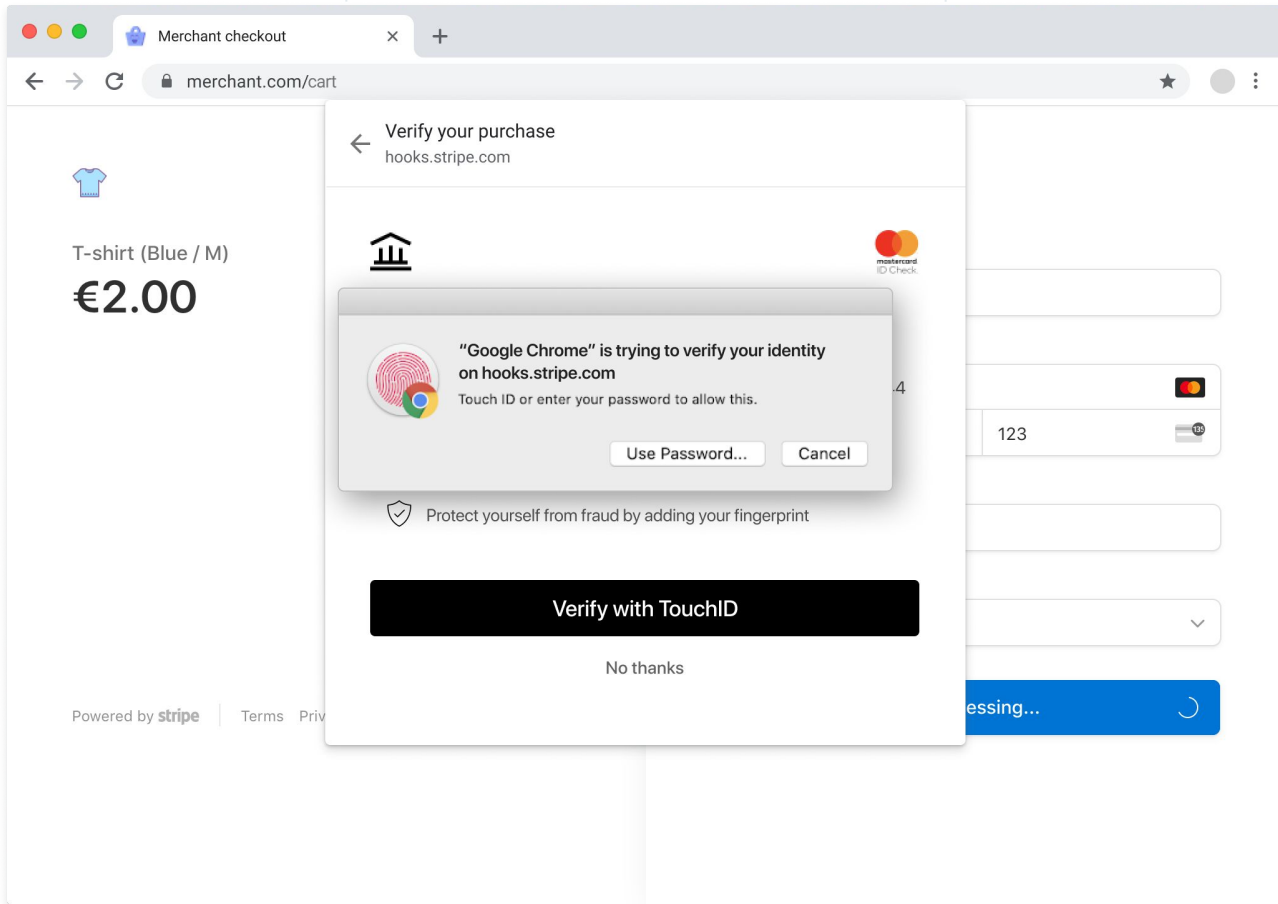


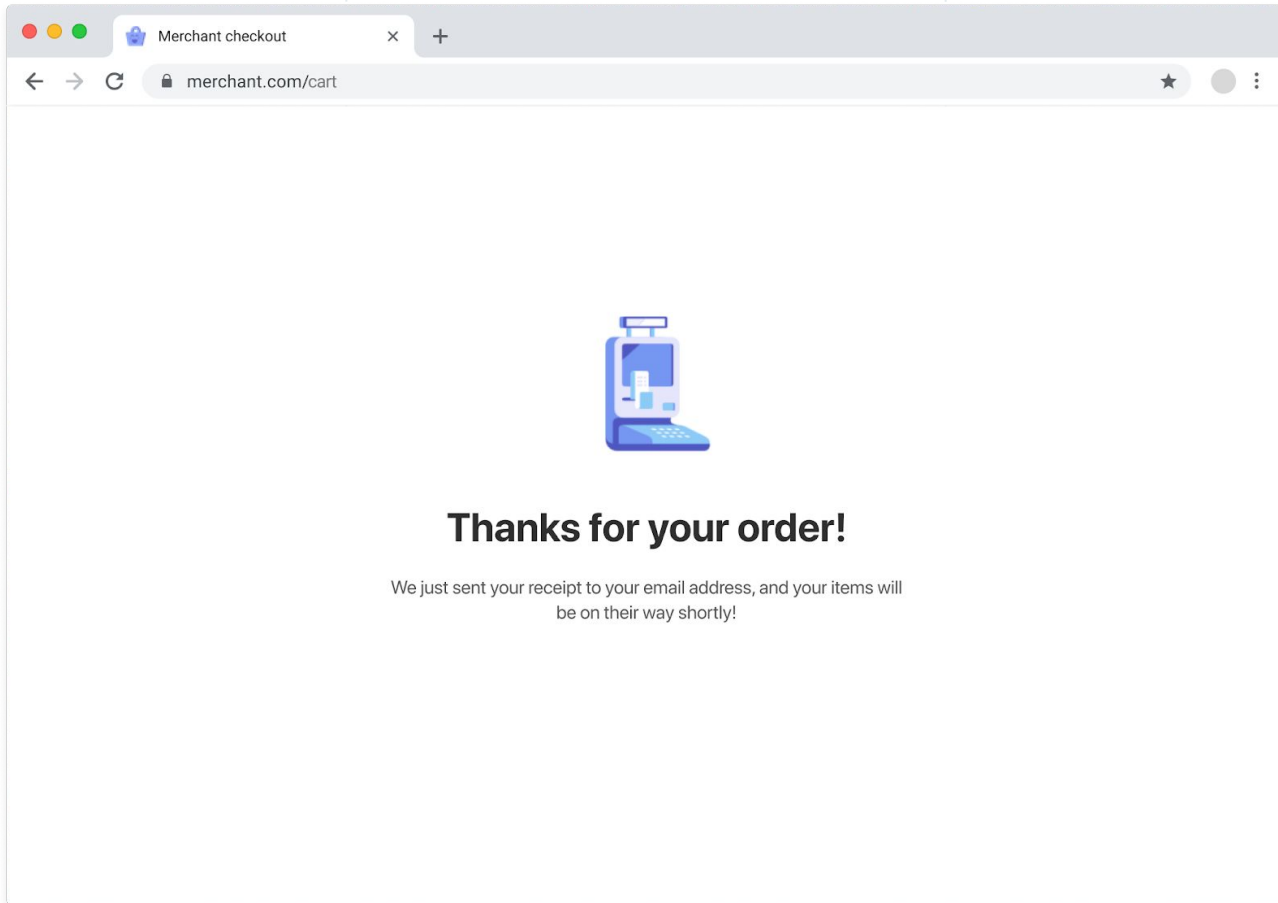
PH window












About the Secure Payment Confirmation API

# Authentication Flow Mocks

Merchant checkout

merchant.com/cart



 T-shirt (Blue / M)  
**€2.00**

Powered by **stripe** | [Terms](#) [Privacy](#)

### Pay with card


Email

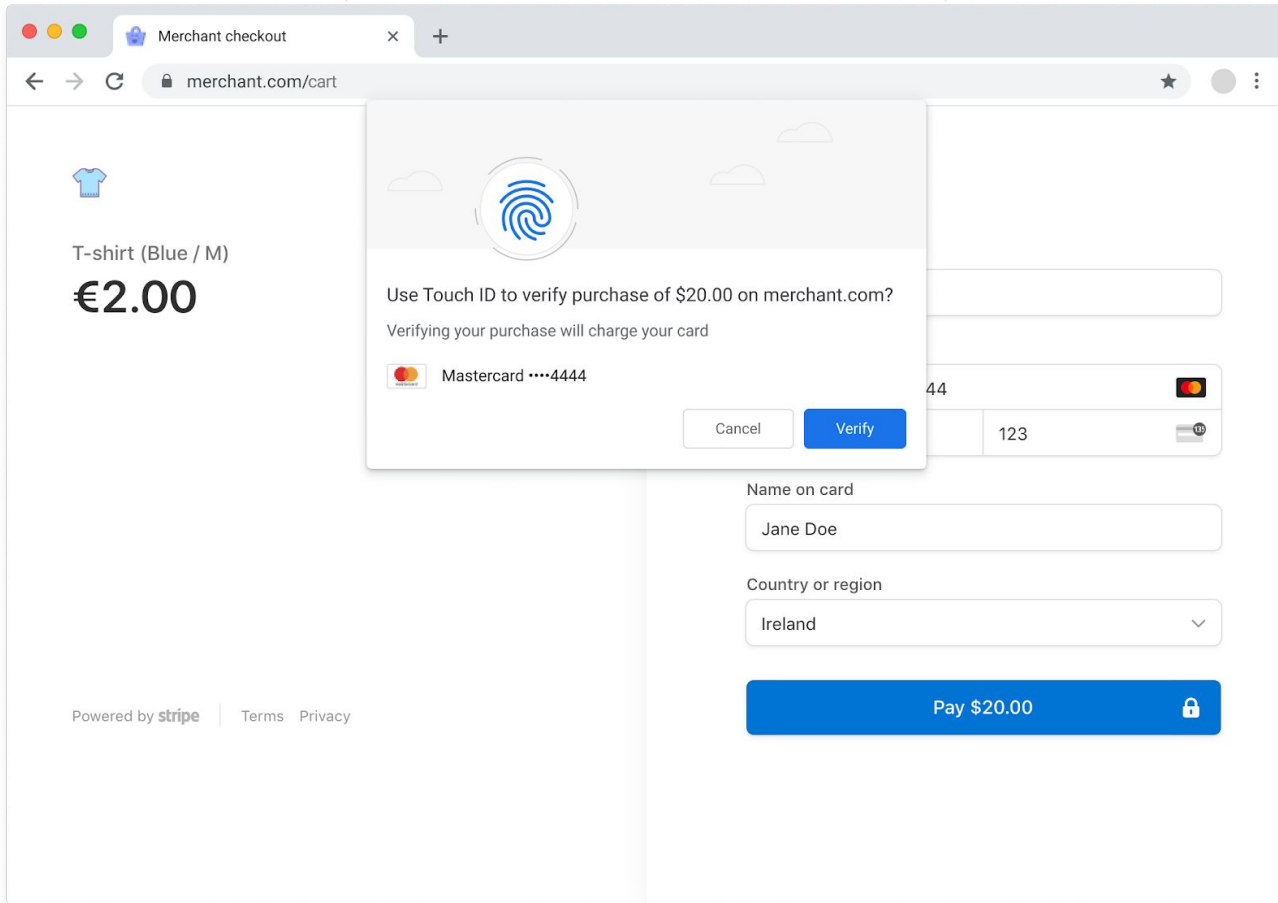
Card information

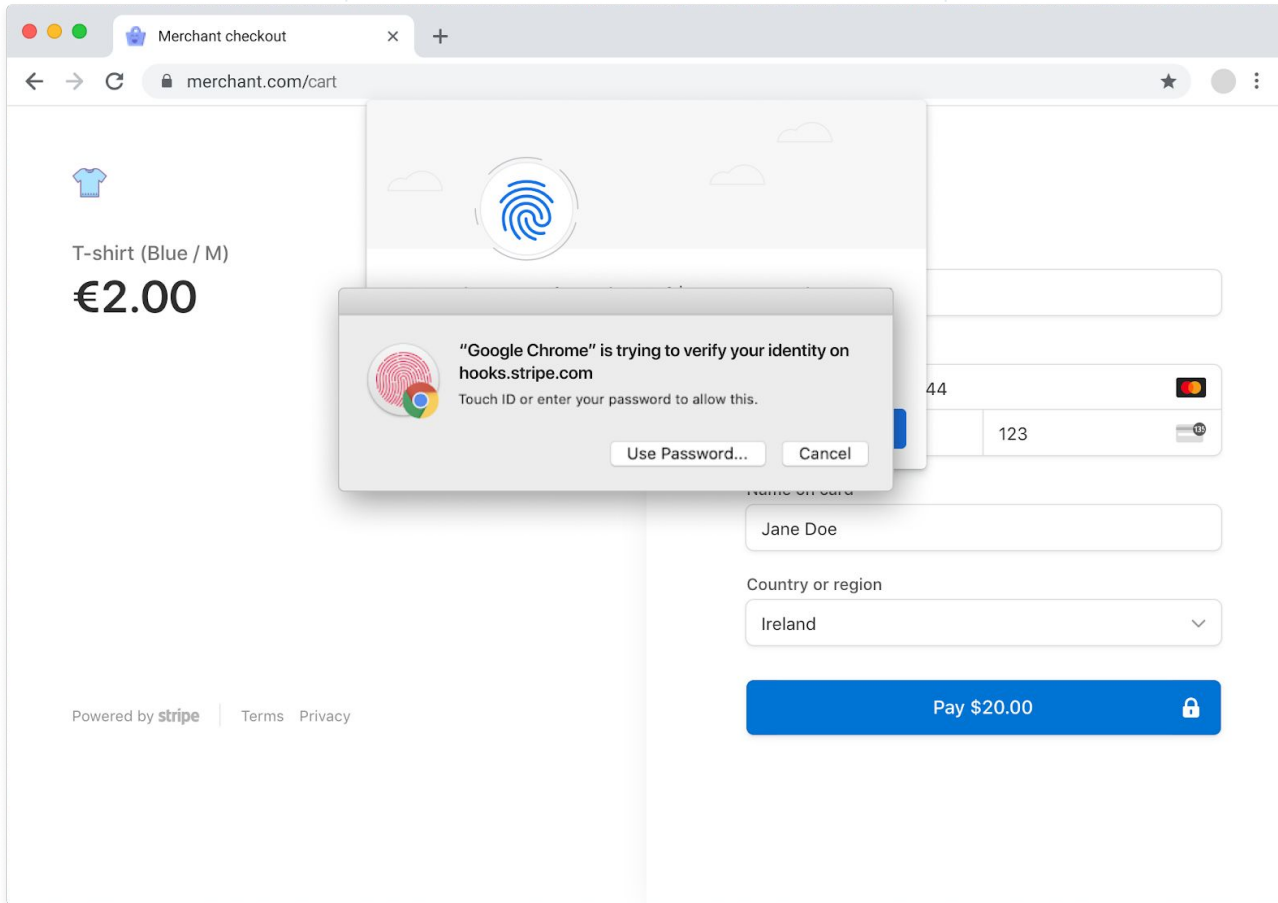
<input type="text" value="5555 5555 5555 4444"/>		
<input type="text" value="01 / 25"/>	<input type="text" value="123"/>	

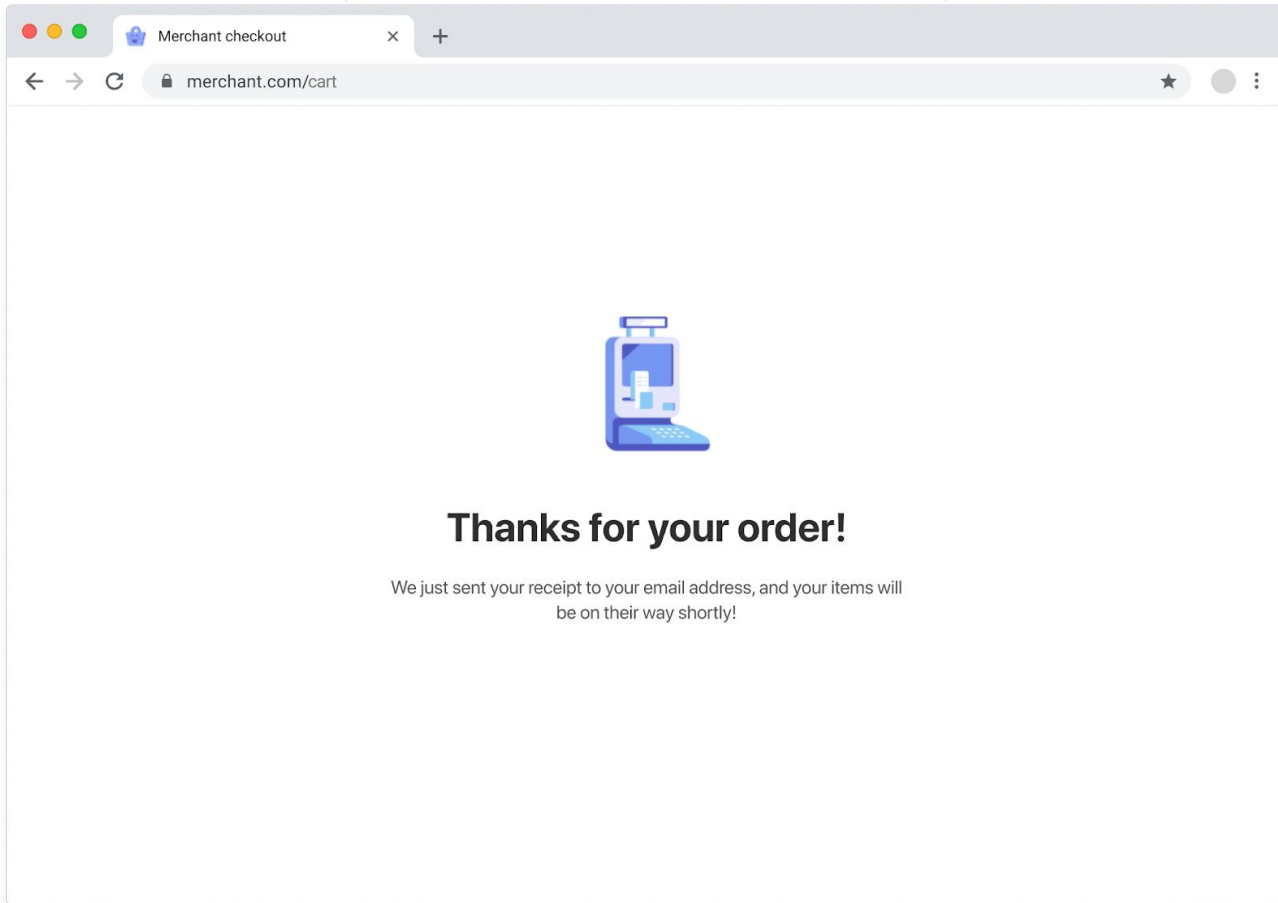
Name on card

Country or region







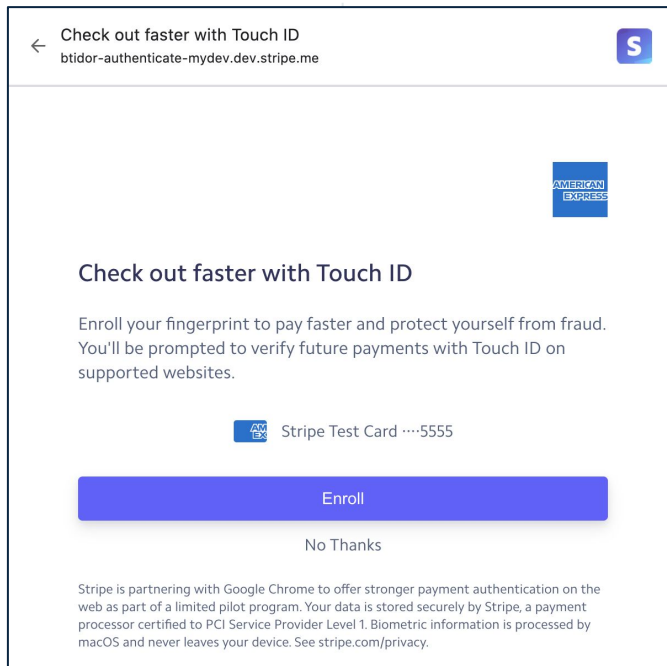


# Enrollment

## Pilot Flow

1. User visits issuing bank, either during a traditional authentication or separately
2. Issuing bank triggers enrollment, provides instrument name and icon
3. Browser returns a **PaymentCredential** (based on **PublicKeyCredential**, keys stored in FIDO U2F internally)
4. Issuing bank, acting as Relying Party, registers public key and instrument ID in their backend

## Pilot UI





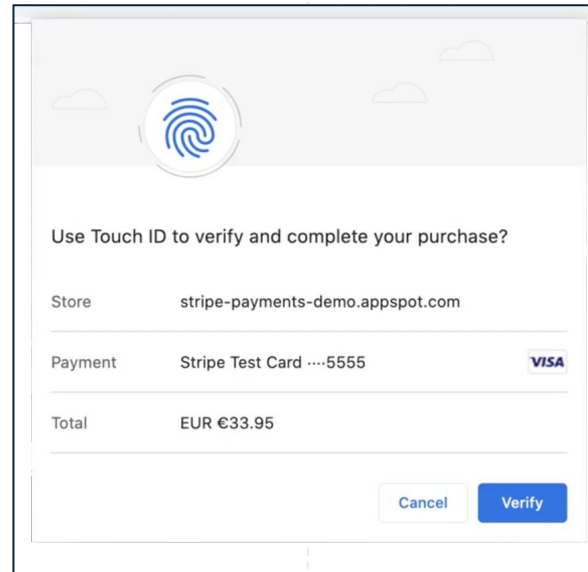
# Authentication

## Pilot Flow

1. Merchant requests list of credential IDs from issuing bank via backend protocol (e.g. 3D Secure)
2. Merchant invokes Payment Request API **on their origin** with instrument IDs and transaction details
3. Browser displays transaction details to user, collects biometric confirmation
4. Browser **binds transaction details into Web Authentication challenge** and returns signed assertion (Web Payment Cryptogram) to merchant
5. Merchant submits Web Payment Cryptogram to issuer via backend protocol **and** can verify the signature independently

stripe

## Pilot UI



# Eligibility Requirements

## Customer

Chrome 86+ on macOS

Has FIDO user-verifying platform authenticator (Touch ID)

Visa, Mastercard and American Express

Card supports 3D Secure 2

Excluded: cards that decline non-3D Secure transactions — India + 3 European countries with early SCA enforcement

## Merchant

Cohort of global internet businesses, predominantly small and medium-sized

## Duration

November 12 to January 25

# Experiment Arms

## 3DS2 Challenge

Trigger 3D Secure 2

Request a challenge from the issuing bank via requestorChallengeInd=03

Run challenge in an iframe

*Benchmark for markets where two-factor authentication is required by law: India + Europe under SCA*

## Vanilla 3DS

Trigger 3D Secure 1 or 2 based on internal optimization logic

Request frictionless flow via requestorChallengeInd=02

If challenged, run challenge in an iframe

*Benchmark for markets where frictionless authentication is prevalent*

## Secure Payment Confirmation

Perform 3D Secure 2

Request a challenge from the issuing bank via requestorChallengeInd=03

Run challenge in a Secure Modal Window

Upon successful completion, prompt user to enroll a credential

Subsequent payments: authenticate with Secure Payment Confirmation + **fall back** to 3D Secure 2 challenge if unsuccessful

# Hypotheses

Secure Payment Confirmation **increases conversion** (authentication rate) compared to other arms

Secure Payment Confirmation **reduces time spent** (authentication duration) compared to other arms

# All-inclusive Conversion

84.7%

## 3DS2 Challenge

**Limitation:** excludes transactions where the issuing bank returned frictionless approval or error (> 50%) — not directly comparable with the Vanilla 3DS arm

91.4%

## Vanilla 3DS

92.7%

## Secure Payment Confirmation

Includes fallback to the 3D Secure 2 challenge flow

**Limitation:** excludes transactions where the issuing bank returned frictionless approval or error (> 50%) — not directly comparable with the Vanilla 3DS arm

# SPC Biometric Flow

## Est. Biometric Confirmation Rate

**86.3%**

Driven by users canceling out of biometric flow, likely due to unfamiliarity as rate increases on subsequent payments.

Even if user cancels, can still recover the payment by completing a traditional 3D Secure challenge.

**Limitation:** some frontend events blocked by ad blockers, rate interpolated

## Enrollment Rate

**20%**

## Fraud Rate

**Negligible**

# Median Duration

**36s**

## 3DS2 Challenge

Mean of 52 seconds

Mean is elevated due to long tail of slow authentications

**7s**

## Vanilla 3DS

Mean of 22 seconds

Mean is elevated due to authentications where the frictionless flow is not granted

**12s**

## Secure Payment Confirmation

Mean of 15 seconds

Mean remains low because fallback to 3D Secure challenge is rare

# Summary

## Key Results

SPC pilot **increases conversion by 8pp** compared with 3DS2 challenge flow

SPC pilot **reduces authentication duration by over 3x** compared with 3DS2 challenge flow


## Future Work

Experimenting with issuer branding and copy changes to improve authentication and enrollment rates

More precise measurement of when and why users fall back from the biometric prompt

Integration with 3D Secure and additional payments protocols

Feedback from stakeholders, developing the design of the API

 **Many thanks to the Google Chrome team for piloting this proposal with us**