Secure Payment Confirmation (SPC)

Doug Fisher

W3C TPAC | Sept 2023

Notice of confidentiality

This presentation is furnished to you solely in your capacity as a customer of Visa Inc. and/or a participant in the Visa payments system. By accepting this presentation, you acknowledge that the information contained herein (the "Information") is confidential and subject to the confidentiality restrictions contained in Visa's operating regulations and/or other confidentiality agreements, which limit your use of the Information. You agree to keep the Information confidential and not to use the Information for any purpose other than in your capacity as a customer of Visa Inc. or as a participant in the Visa payments system. The Information may only be disseminated within your organization on a need-to-know basis to enable your participation in the Visa payments system. Please be advised that the Information may constitute material non public information under U.S. federal securities laws and that purchasing or selling securities of Visa Inc. while being aware of material non public information would constitute a violation of applicable U.S. federal securities laws.

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 Information 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.

This presentation includes programs, concepts and details under continuing development by Visa. Any Visa features, functionality, implementation, branding, and schedules may be amended, updated or canceled at Visa's discretion. The timing of widespread availability of programs and functionality is also subject to a number of factors outside Visa's control, including but not limited to deployment of necessary infrastructure by issuers, acquirers, merchants and mobile device manufacturers. In addition, certain existing features are not available in all countries. Participation in programs and services are subject to Visa's terms and conditions in program participation agreements and associated documentation.

Forward-looking statements and disclaimer

This presentation may contain forward-looking statements within the meaning of the U.S. Private Securities Litigation Reform Act of 1995. These statements can be identified by the terms "objective," "goal," "strategy," "opportunities," "continue," "can," "will" and other similar references to the future. Examples of such forward-looking statements may include, but are not limited to, statements we make about our corporate strategy and product goals, plans and objectives. By their nature, forward-looking statements: (i) speak only as of the date they are made, (ii) are neither statements of historical fact nor guarantees of future performance and (iii) are subject to risks, uncertainties, assumptions and changes in circumstances that are difficult to predict or quantify. Therefore, actual results could differ materially and adversely from those forward-looking statements because of a variety of factors, including the following: macroeconomic and industry factors such as currency exchange rates, global economic, political, health and other conditions, competitive pressure on customer pricing and in the payments industry generally, material changes in our customers' performance compared to our estimates; systemic developments such as disruption of our transaction processing systems or the inability to process transactions efficiently, account data breaches involving card data stored by us or third parties, increased fraudulent and other illegal activity involving our cards; and the other factors discussed under the heading "Risk Factors" in our most recent Annual Report on Form 10-K and our most recent Quarterly Reports on Form 10-Q. You should not place undue reliance on such statements. Unless required to do so by law, we do not intend to update or revise any forward-looking statement, because of new information or future developments or otherwise.

Studies, survey results, research, recommendations, and opportunity assessments are provided for informational purposes only and should not be relied upon for marketing, legal, regulatory or other advice. Recommendations and opportunities 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 any studies, survey results, research, recommendations, opportunity assessments, or other information, including errors of any kind, or any assumptions or conclusions you might draw from their use. Except where statistically significant differences are specifically noted, survey results should be considered directional only.

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.

This material shall not constitute a Submission, as defined and used in the W3C Patent Policy and Process Document.

of programs and functionality is also subject to a number of factors outside Visa's control, including but not limited to deployment of necesThis presentation includes programs, concepts and details under continuing development by Visa. Depictions may be illustrative only and capabilities and features may require development, implementation and resources by you based on your business and operational details. Participation, prototyping or collaboration activities are subject to Visa's additional terms and conditions. Any Visa features, functionality, implementation, branding, and schedules may be amended, updated or canceled at Visa's discretion. The timing of widespread availabilitysary infrastructure by issuers, acquirers, merchants and mobile device manufacturers. In addition, certain existing features are not available in all countries.

Participation in programs and services are subject to Visa's terms and conditions in program participation agreements and associated documentation. Visa does not provide legal, regulatory, tax or financial advice; you are responsible for conducting your own legal and regulatory due diligence, analyses and compliance. For avoidance of doubt, no exclusivity is provided by Visa to you associated with the Information, concepts or materials related to this discussion.

Agenda

1

SPC pilot update

2

SPC usability findings
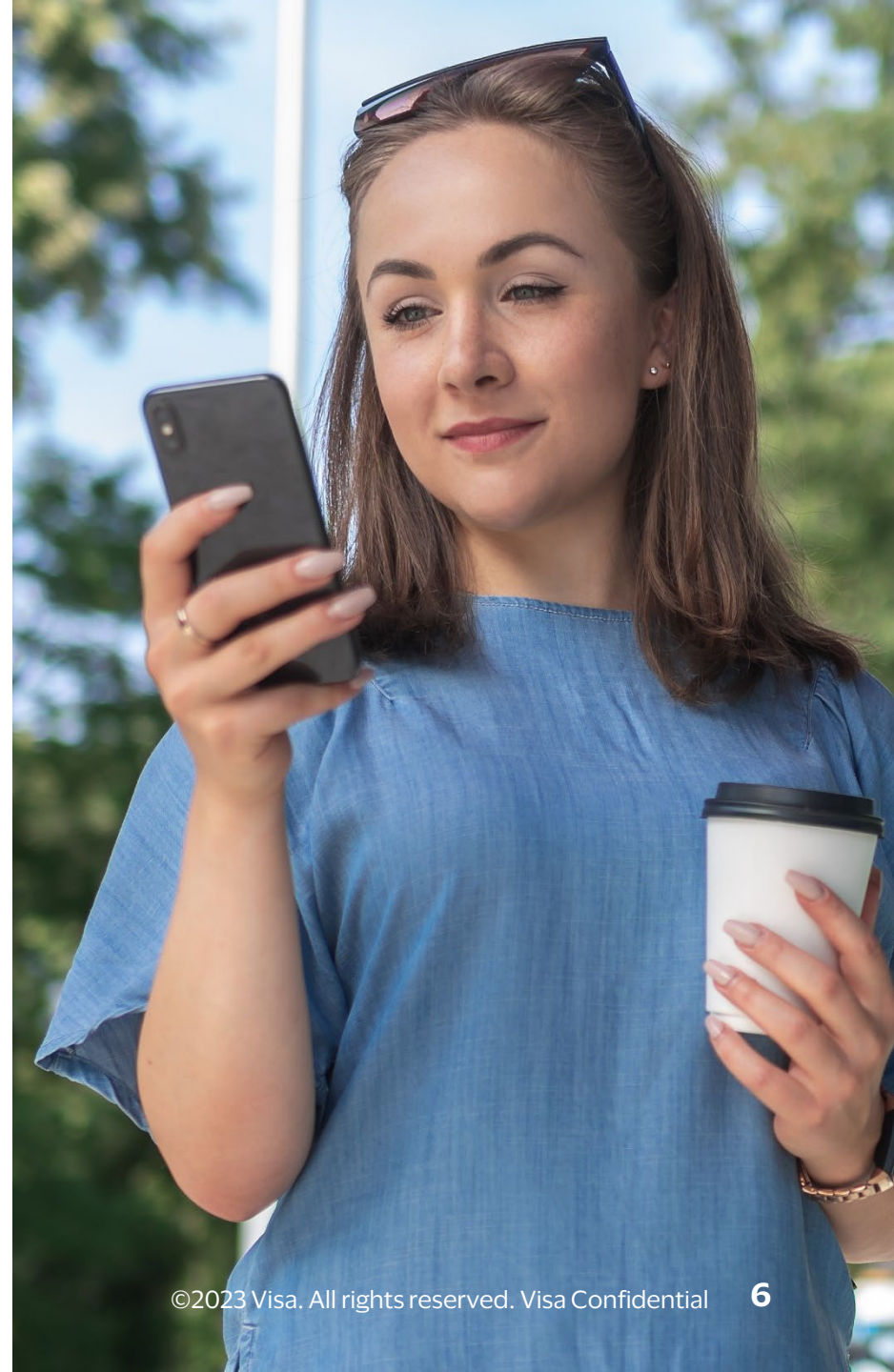
3

SPC vs OTP UX comparison
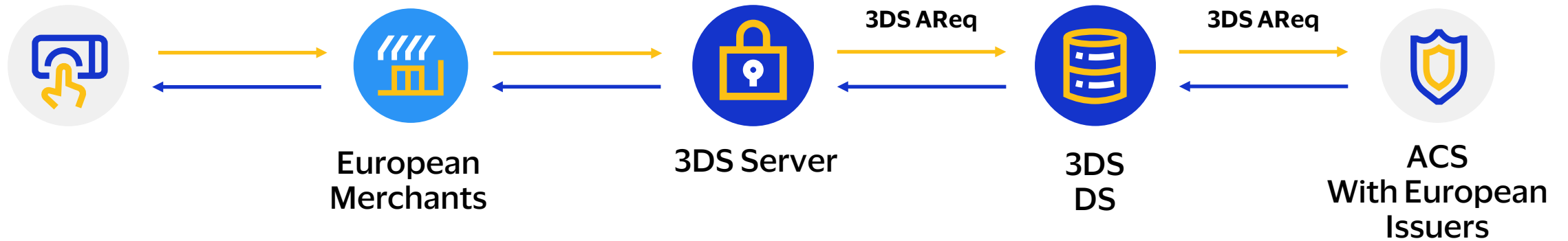
4

SDemo slides

SPC Pilot Update

Pilot background

- W3C published SPC as a Candidate Recommendation on June 15, 2023

- Visa is piloting SPC to obtain implementation experience with the SPC Candidate Recommendation

- The pilot covers the payment use case with 3DS and with merchant initiated SPC where the issuer is the relying party

- The objective is to obtain feedback on any barriers that would prevent SPC from scaling globally from the consumer and technical perspectives

VISA

Visa is conducting two SPC pilots in parallel

European Merchants → 3DS Server → **3DS AReq** → 3DS DS → **3DS AReq** → ACS With European Issuers

Phase 1 is underway with friends, family and selected consumers.

Phase 2 will be limited BIN range in a production environment.

Both Phases of the pilots cover enrollment and authentication flows

SPC is being piloted with 3DS 2.3.1.1

Displayed by browser

Consumer   **Merchant**   **3DS Server**   **DS**   **ACS**

3DS Requestor SPC Support = Y, if SPC supported

3DS Requestor invokes the SPC authentication against the Credentials returned by the ACS

Transaction Status = S
WebAuthn Credential list and UI elements

Transaction Status = S
WebAuthn Credential list and UI elements

The 3DS Requestor initiates a second 3DS AReq to pass the result of the SPC authentication to the ACS

FIDO Assertion   FIDO Assertion
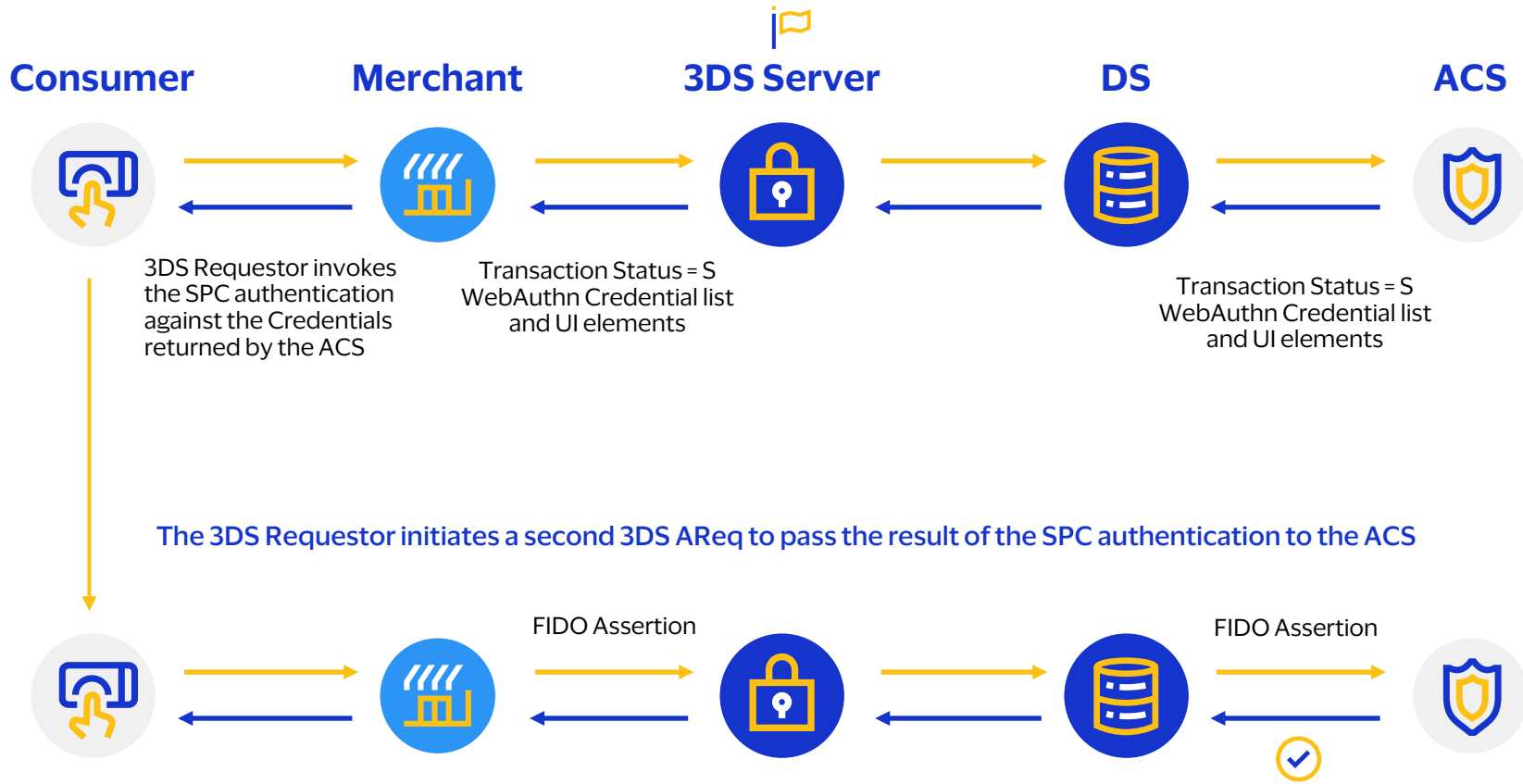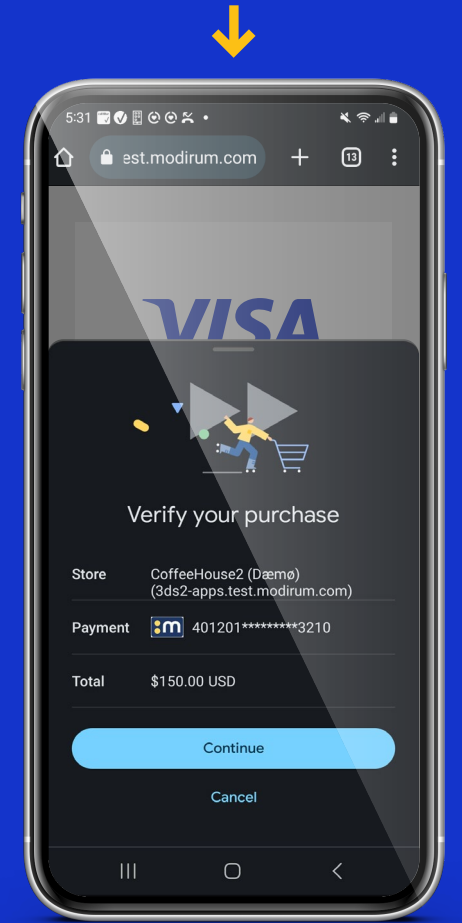
Netcetera providing 2.3.1.1. components

Verify your purchase

Store	CoffeeHouse2 (Dæmø) (3ds2-apps.test.modirum.com)
Payment	401201*********3210
Total	$150.00 USD

Continue

Cancel

VISA

SPC is also being piloted with 3DS 2.2 with an extension

3DS Requestor SPC Support = Y, if SPC supported

Consumer	Merchant	3DS Server	DS	ACS

3DS Requestor invokes the SPC authentication against the Credentials returned by the ACS

Transaction Status = S
WebAuthn Credential list and UI elements

Transaction Status = S
WebAuthn Credential list and UI elements

The 3DS Requestor initiates a second 3DS AReq to pass the result of the SPC authentication to the ACS

FIDO Assertion

FIDO Assertion

Modirum providing 2.2 components and extension

Displayed by browser

5:31   est.modirum.com

VISA

Verify your purchase

Store	CoffeeHouse2 (Dæmø) (3ds2-apps.test.modirum.com)
Payment	401201*********3210
Total	$150.00 USD

Continue

Cancel
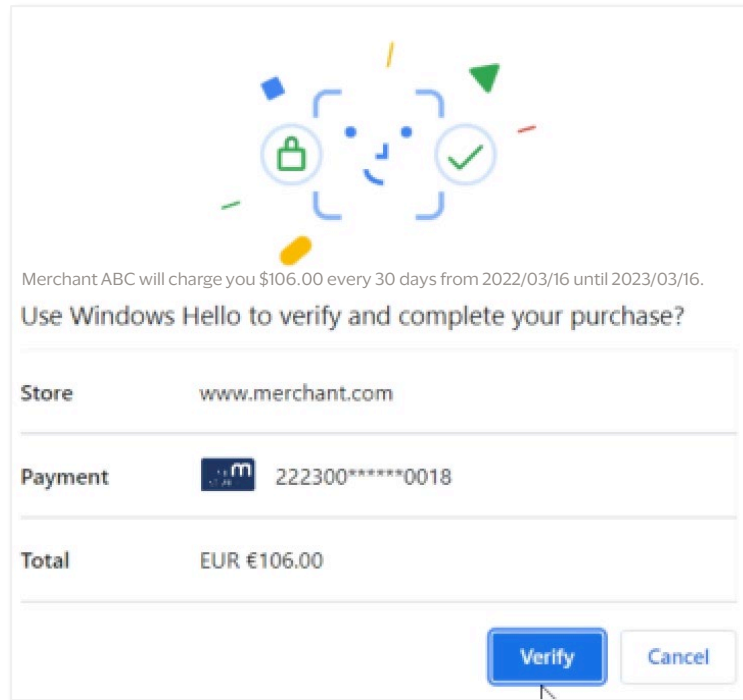
SPC Usability Study
Consumer feedback on SPC UI is being obtained

BUSINESS GOALS

Evaluate UI options to improve seamlessness

- Branding / value of logos
- Alternative wording of consumer instructions
- Known merchant name vs. URL
- Card art size

TECHNICAL GOALS

Capture data to allow usability study analysis

Compare to other 3DS challenge methods

SPC authentication would be tested against other standard
3DS challenge (e.g. SMS, OOB) and also native WebAuthn

ACS
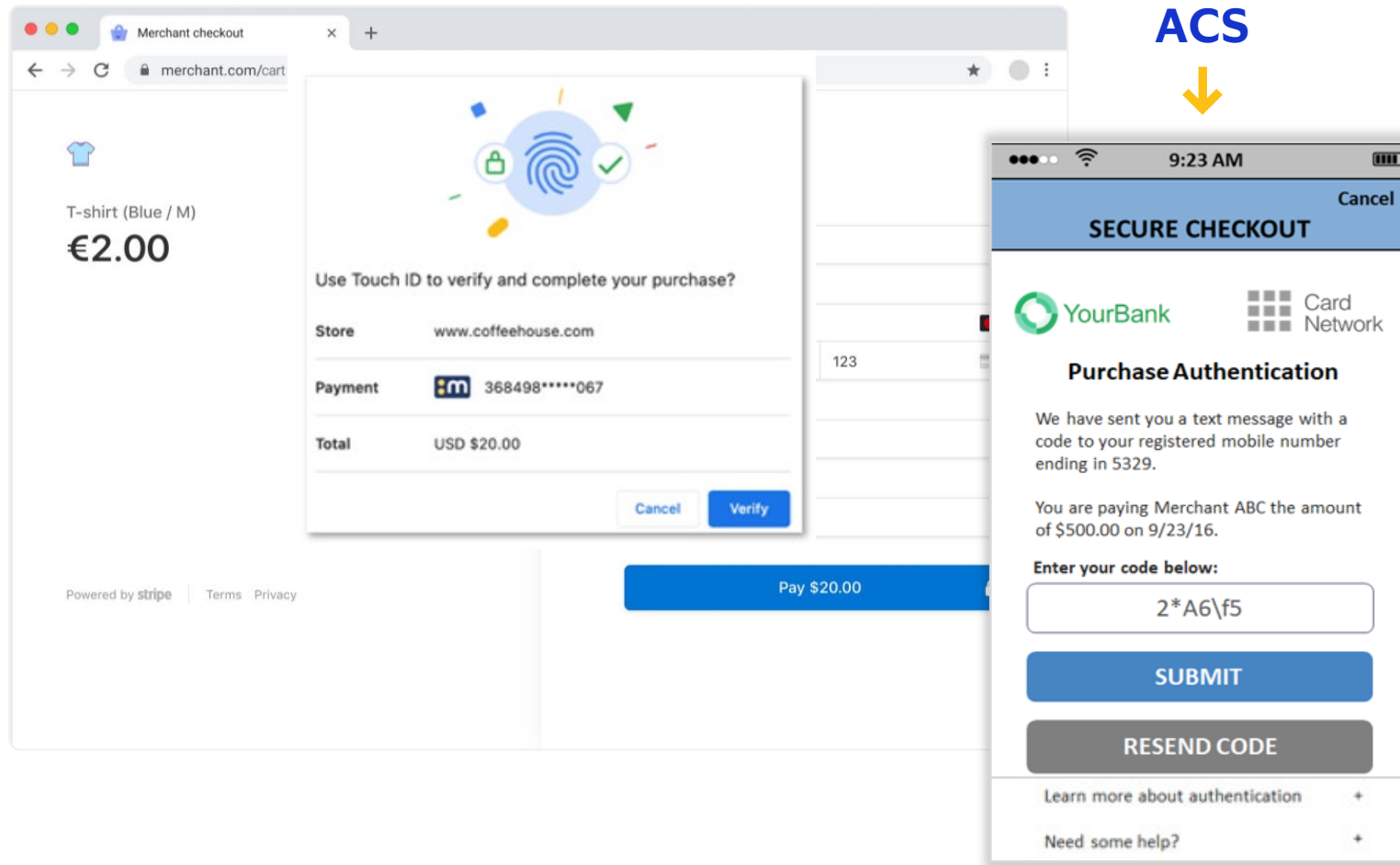
BUSINESS GOALS

- Evaluate consumers auth preferences
- Evaluate pros/cons of methods
- Evaluate timing vs. standard 3DS methods
- Evaluate completion rates
- Measure SPC to other authentication methods that require a separate device to authenticate
- Evaluate UI options to improve success rates

TECHNICAL GOALS

- Pilot portal supports analysis of alternative authentication methods
- Test WebAuthn on non-SPC supporting browser

SPC with fallback 3DS challenge transaction

SPC authentication would interact with a 3DS challenge if consumer hits cancel, timeouts, etc. Evaluate branding importance

ACS
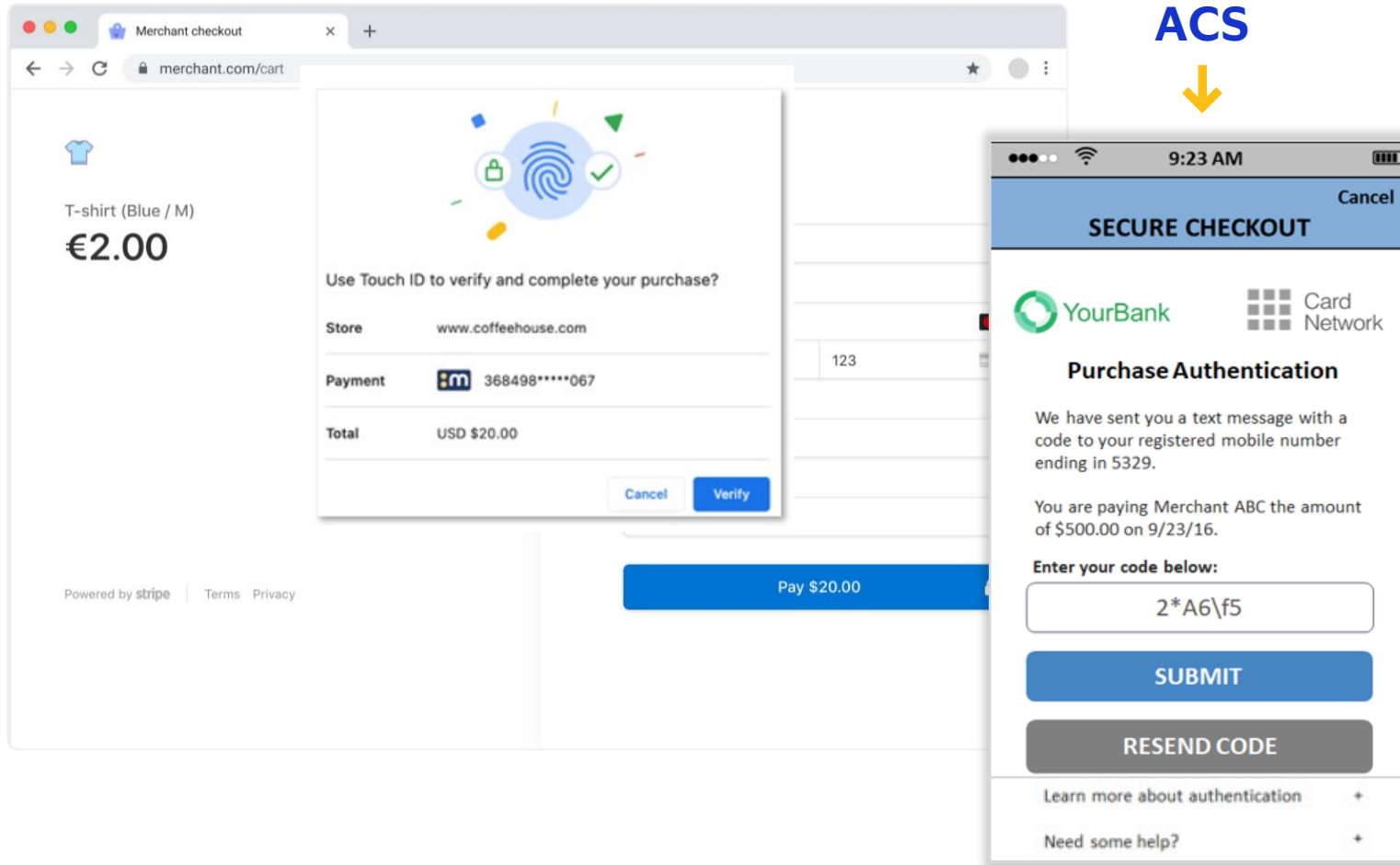
BUSINESS GOALS

- Do consumers understand change in context between browser chrome UI vs 3DS UI?
- Evaluate UI options to improve seamlessness
- Evaluate timing vs. standard 3DS

TECHNICAL GOALS

- Prove fallback flows work

SPC Usability Findings

Objectives

- Gather feedback on initial reaction to encountering SPC in both enrollment and authentication flows

- Investigate whether participants can successfully and easily enroll in SPC

- Identify potential content and usability improvements to the enrollment and authentication flows

Research Questions

- Do users understand the value proposition of SPC when prompted after a 3DS flow?

- Is the enrollment flow easy for participants to follow? Is there any information users are looking for that is not included?

- Do users understand what they have enrolled for? In the future, how do users expect to interact with SPC?

- How do users react to SPC in an authentication flow, and are there any potential usability issues?

Flows Tested

Enrollment Flow
Enrollment subsequent to 3DS

SPC Authentication
Transaction using SPC

Fallback to 3DS
Fallback flow if user cancels out of SPC

Users need more context and explanation of the value proposition

Based on the screen presented, many participants struggled to understand what they were being asked to do and why.

They often **failed to understand the value of SPC** and **formed inaccurate mental models**, including belief that:

- They were registering for quicker checkout on that website only.
- Their bank was registering a new device after a first-time use of the card from that laptop (not related to browser).

In terms of value proposition, convenience and security are both important – to varying degrees, depending on the individual – but were not adequately explained. Participants did not click 'Learn more'.

SPC Enrollment after 3DS

Confusion with the passkey dialog box

This step was confusing to participants because most of them were unfamiliar with passkeys and were left guessing about what they were being asked and what would happen next. Despite the lack of understanding, most participants would still hit continue.

- One participant believed she would need to save this 'password' for future use.

Create a passkey for 3ds-acs.test.modirum.com

2384f48c-51e2-4f23-8ceb-83a43b7a4441

This passkey will only be saved on this device

Cancel   Continue

Registering device credential. Please wait...

REGISTER YOUR DEVICE

CANCEL REGISTRATION

SPC Authentication Flow

Authentication choice: SPC vs OTP

Some participants did not know what OTP was and chose to authenticate via device because they felt they knew what to expect. Others preferred to authenticate via device so they can stay on one device.

Recommendation: This dialog is confusing and unnecessary from a user perspective and should be removed as soon as possible.

Permission to verify using biometric: Chrome dialog

Most users were expecting to be asked for their biometric at this step, but there was some confusion regarding the 'Verify' button on this screen.

Some participants had expected to be taken directly to the biometric step, therefore the need to click 'Verify' seemed superfluous, with some these participants attempting to use their fingerprint scanner at this point (prior to clicking 'Verify').

Device and OS differences started to come into play here. See subsequent slides.

19
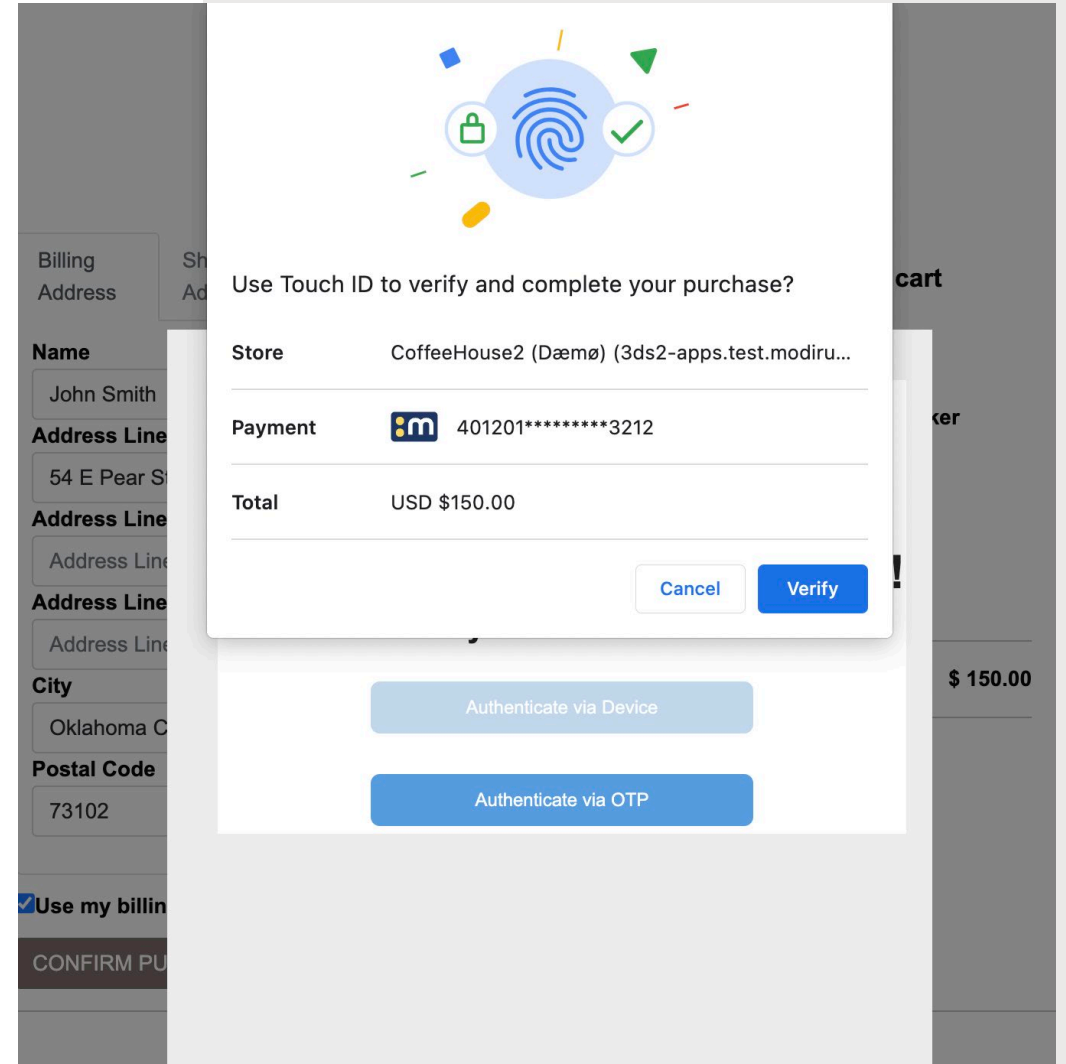
SPC Authentication Flow

Mac - TouchID

Mac participants in the sample seemed well-acquainted with Touch ID and the associated dialogs, thus knew to use the fingerprint sensor at the right time.

The fingerprint on the Chrome dialog also seemed helpful in setting proper expectations:
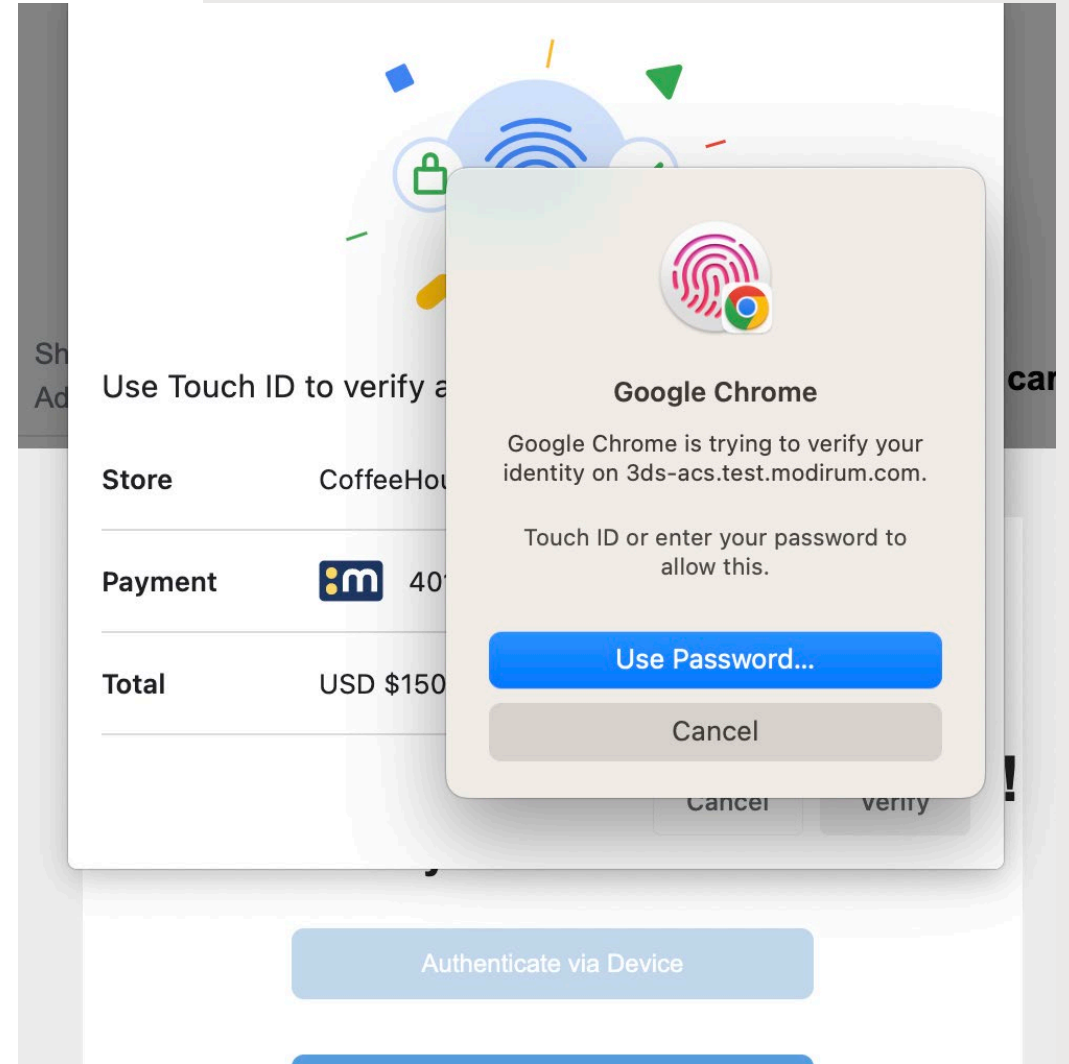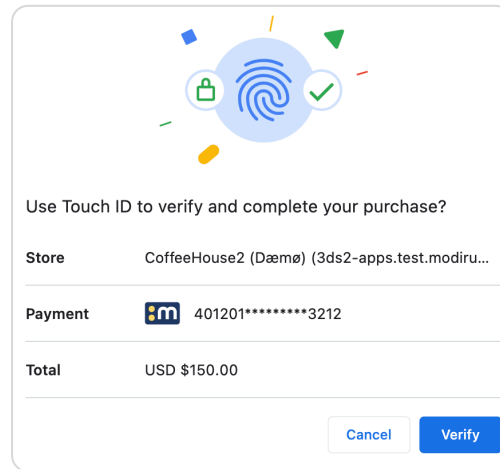
Windows Hello

Windows users in the sample were far less familiar with Windows Hello.

This even included the term 'Windows Hello'. One user who used a fingerprint sensor on his PC was still unfamiliar with the term. The use of 'hello' combined with the face graphic in the Chrome dialog led him to believe the system wanted to use some form of voice recognition.

Lack of familiarity with Windows Hello amongst Windows users could increase potential comprehension and usability issues.

Amongst participants' PCs, Chrome showed the face graphic regardless of the method Windows Hello was using.
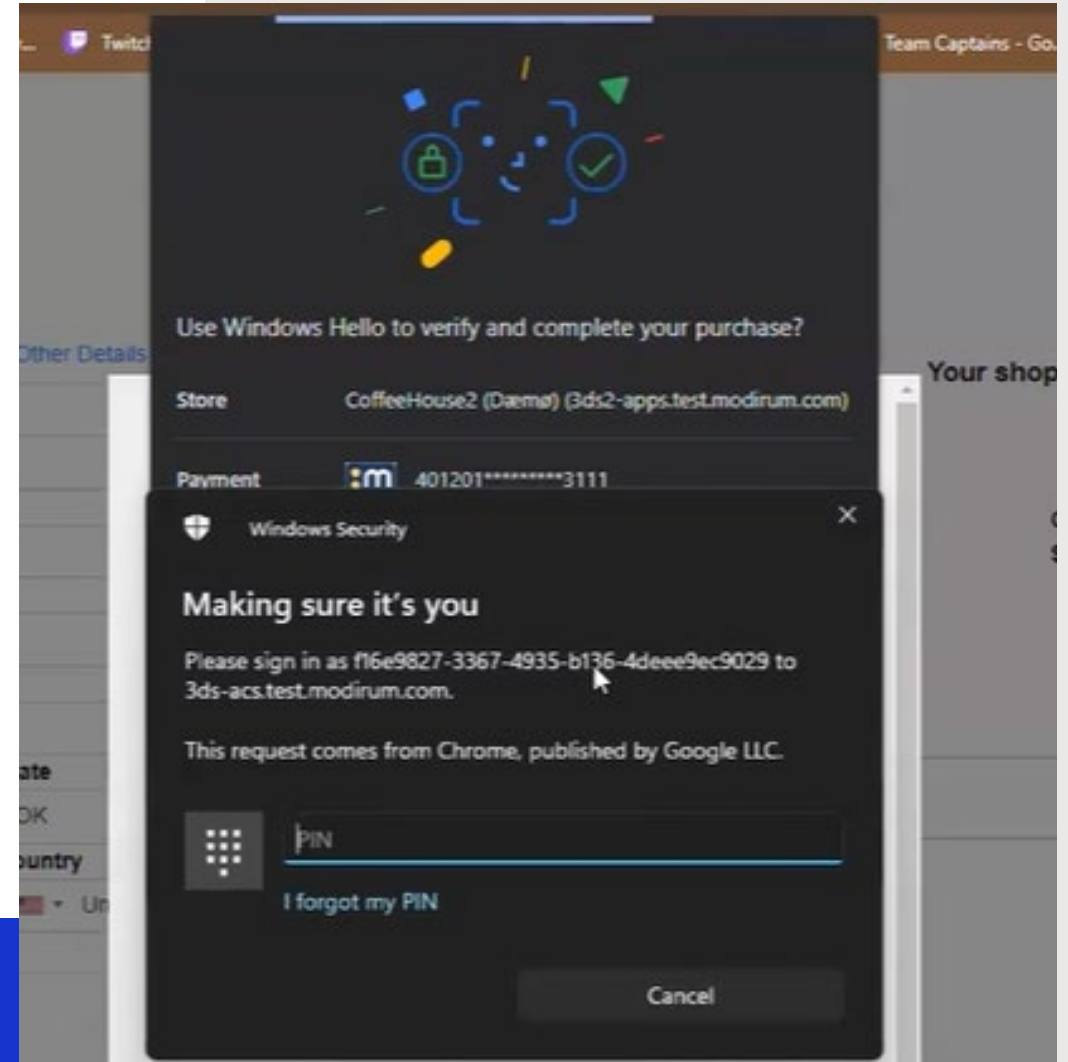
Windows Hello

In addition, the UI of the Windows dialogs caused problems for a few participants.

One participant's PC defaulted to PIN, and the participant failed to see how to switch to a different method (the 'More choices' link) until the moderator was forced to point it out.
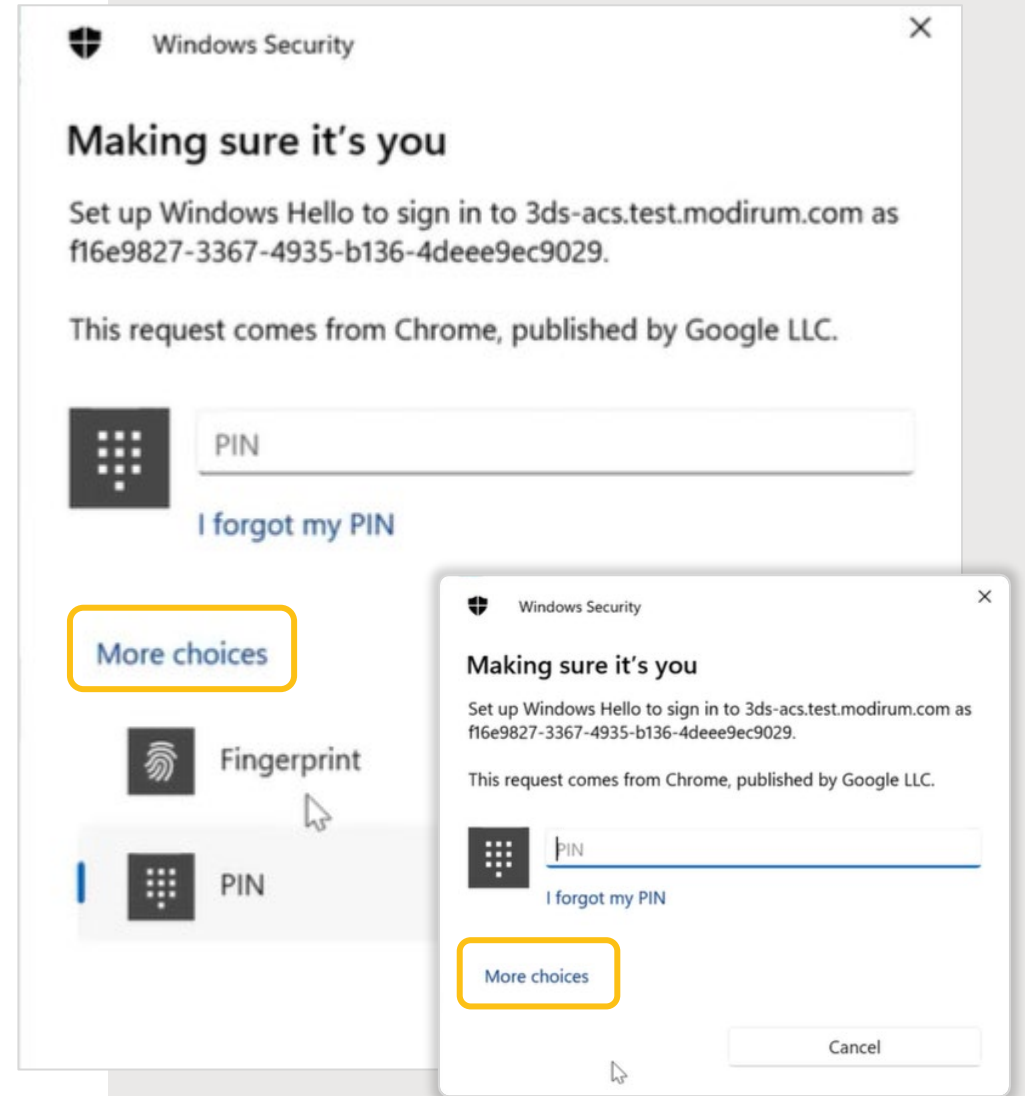
Cancelling biometric authentication

When asked about expectations for what would happen upon cancelling SPC, some participants expected to be taken to the previous page with the two authentication options. Others were concerned that the transaction itself would be cancelled.

Although most participants were not expecting to go directly to the 3DS OTP method, once they experienced it, they stated that it made sense.
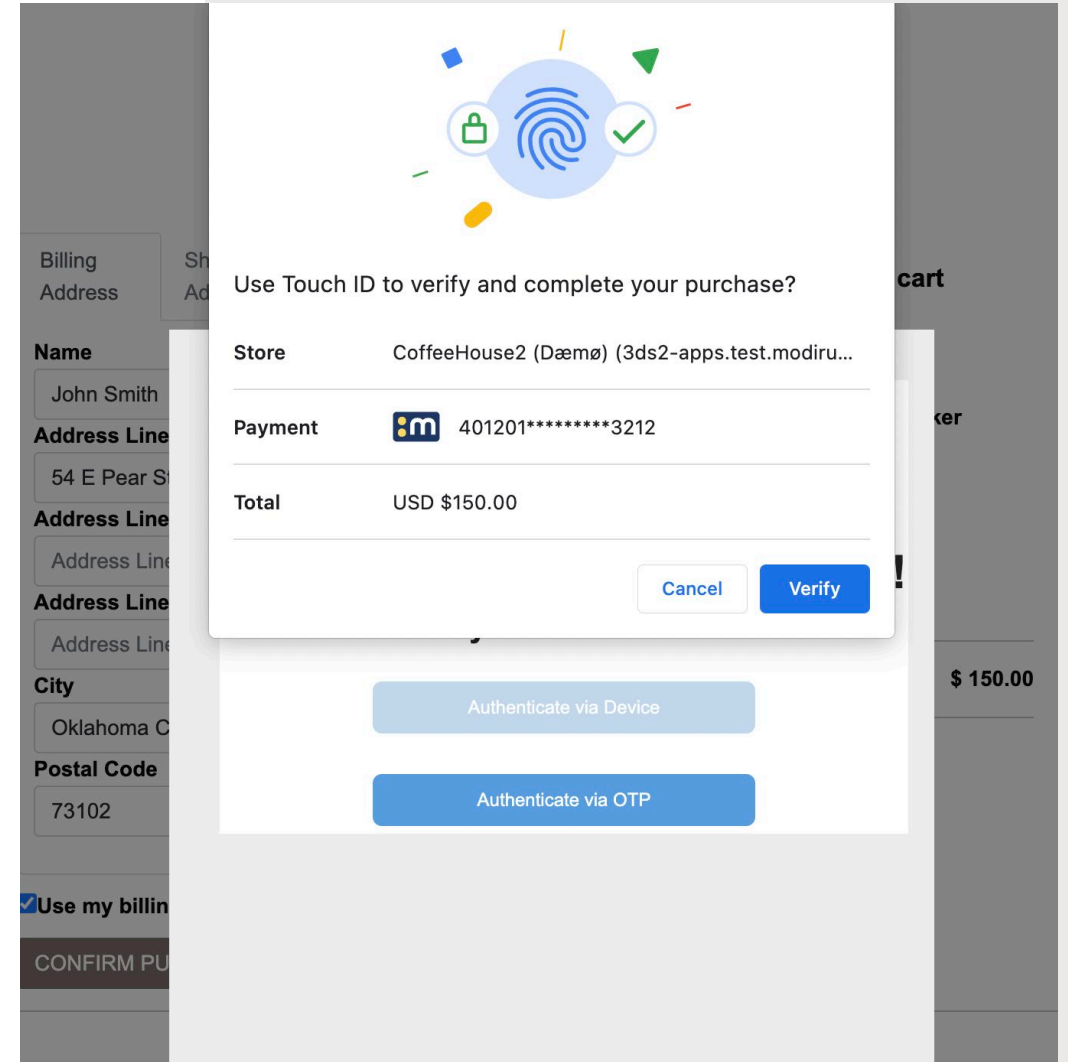
General Findings

Generally positive sentiments towards biometrics

Overall, participants ranked the authentication flow using SPC to be extremely easy, and had positive reactions to using biometrics to authenticate.

Participants mentioned that using biometrics feels secure, fast, and removes the need for using an additional device.

General Findings

Details matter. Use of familiar patterns and conventions aids trust.

Relatively subtle details made a difference. Thus the nuances of copy, labelling, imagery, and flow need to be carefully crafted. Each of these needs work.

As an example, participants were fairly well accustomed to the 3DS steps, and these familiar-looking screens caused no confusion or alarm. For example, cues like issuer and network logos are an important part of trust and security signaling (as per 3DS UX Guidelines which are based on previous research).

Lack of consistency across OSes, devices, and browsers a potential adoption and usability issue

Previous research, both in and out of the electronic payments realm, has demonstrated the importance of consistency for learnability, usability, and building familiarity and trust in a solution. At present this is a potential barrier to adoption and use.

Source placeholder

General Recommendation

Iterative content and interaction design work, as part of a holistic exploration of the overall user flows.

Along with providing insights into technology implementation, using the technical pilot with consumers has demonstrated the need for iterative content & interaction design work on the various touchpoints.

There are **nuances across the various SPC screens, browser integrations, and OS integrations** that should be explored and tested iteratively, in a **holistic fashion that involves all players in the ecosystem**.

This should include further investigation into the potential of post-3DS enrollment.

Iterative design and UX work should be done prior to measuring reactions, preferences, and behaviors in any quantitative fashion in a live environment.

VISA

SPC vs OTP UX comparison

# Comparing SPC and OTP authentication
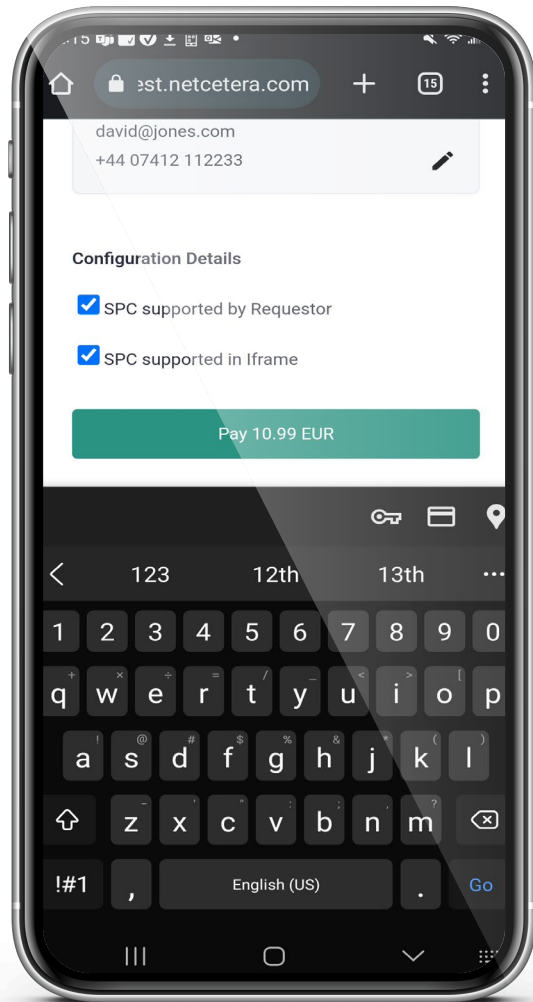
SPC
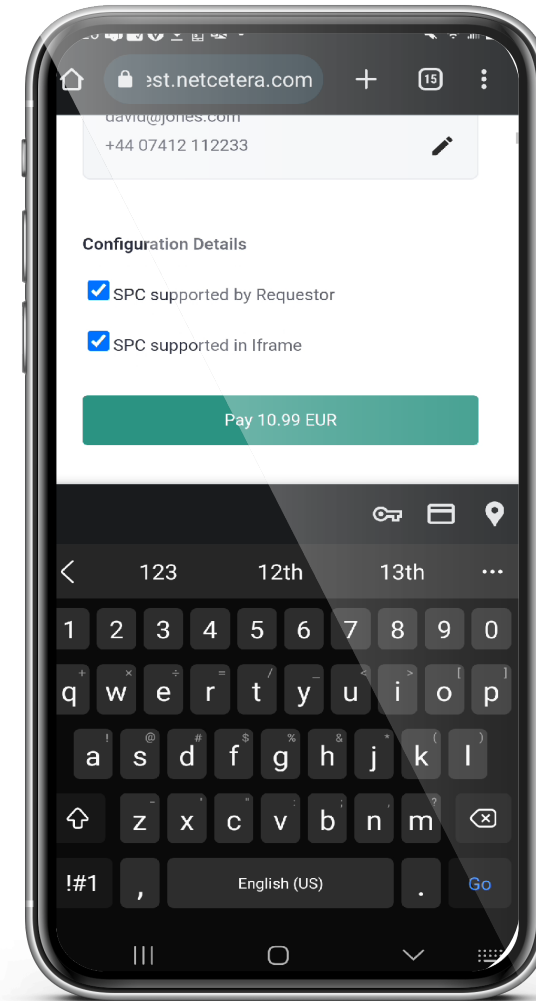
OTP

SPC Demo

Online Shopping begins...

Today let's complete an eCommerce transaction.
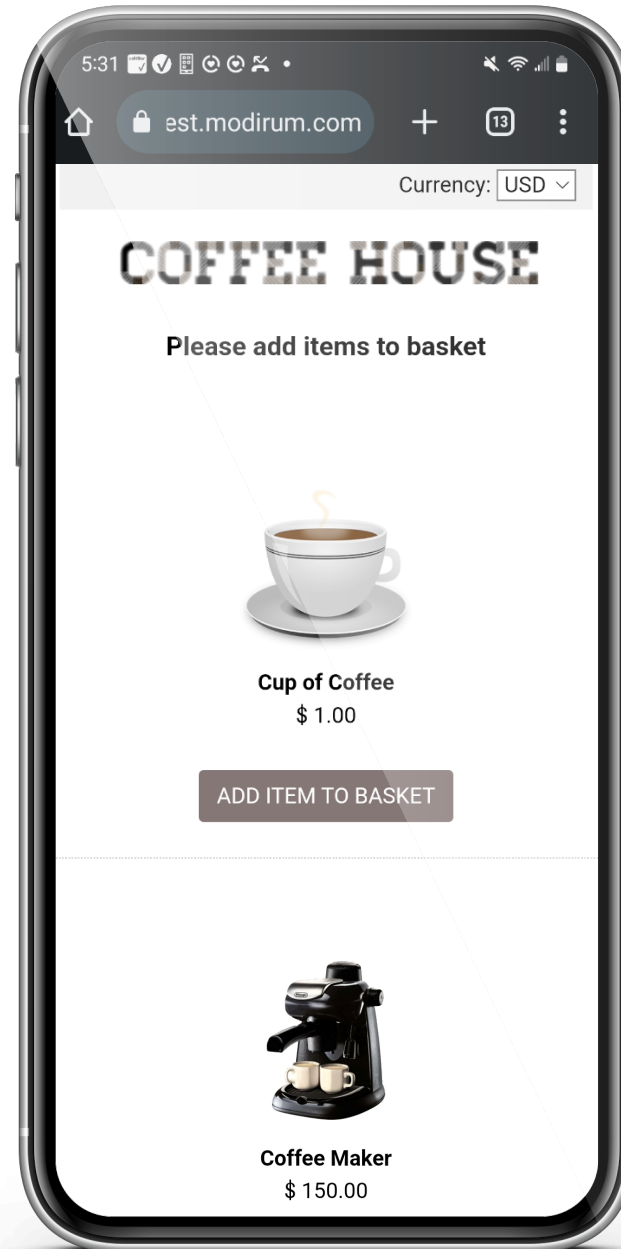
Looking for an item to purchase

In this example, I plan to buy a new coffee maker.
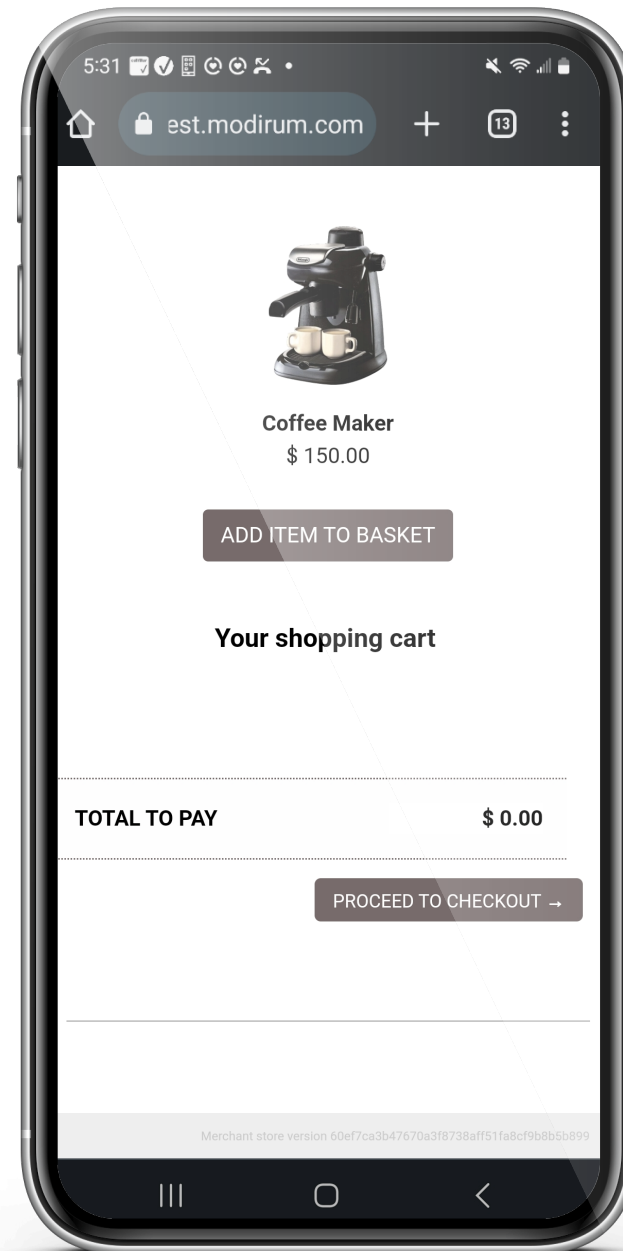
Item is added to the basket

Once the coffee maker is added to my basket, I will proceed with the purchase.
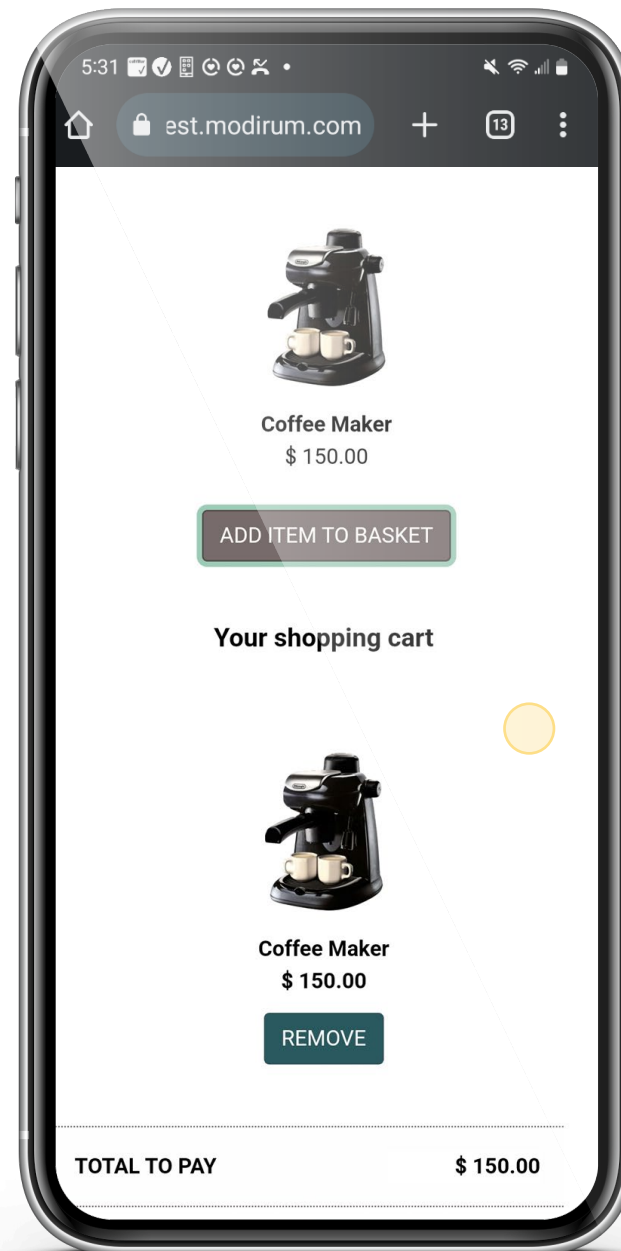
Proceeding to checkout

After the checkout button is clicked, I will start the payment process.
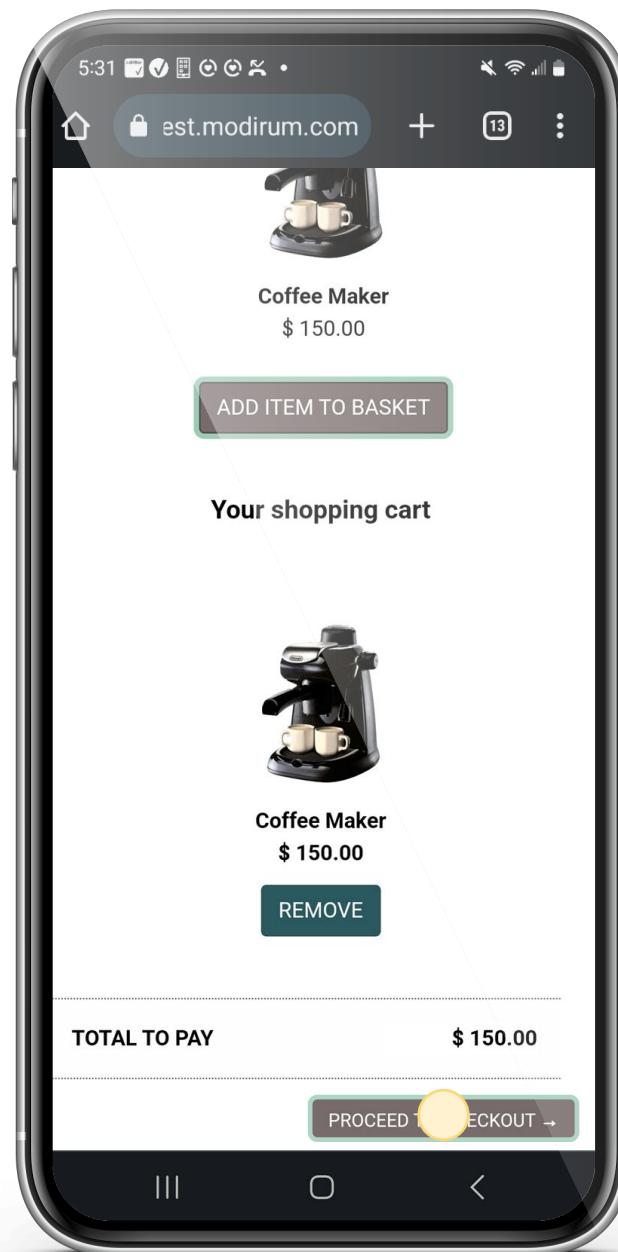
Input of payment details

Card details are entered into the payment screen.

Initiating the purchase

After contact, billing, and shipping address is entered, the shopper clicks the Purchase button.
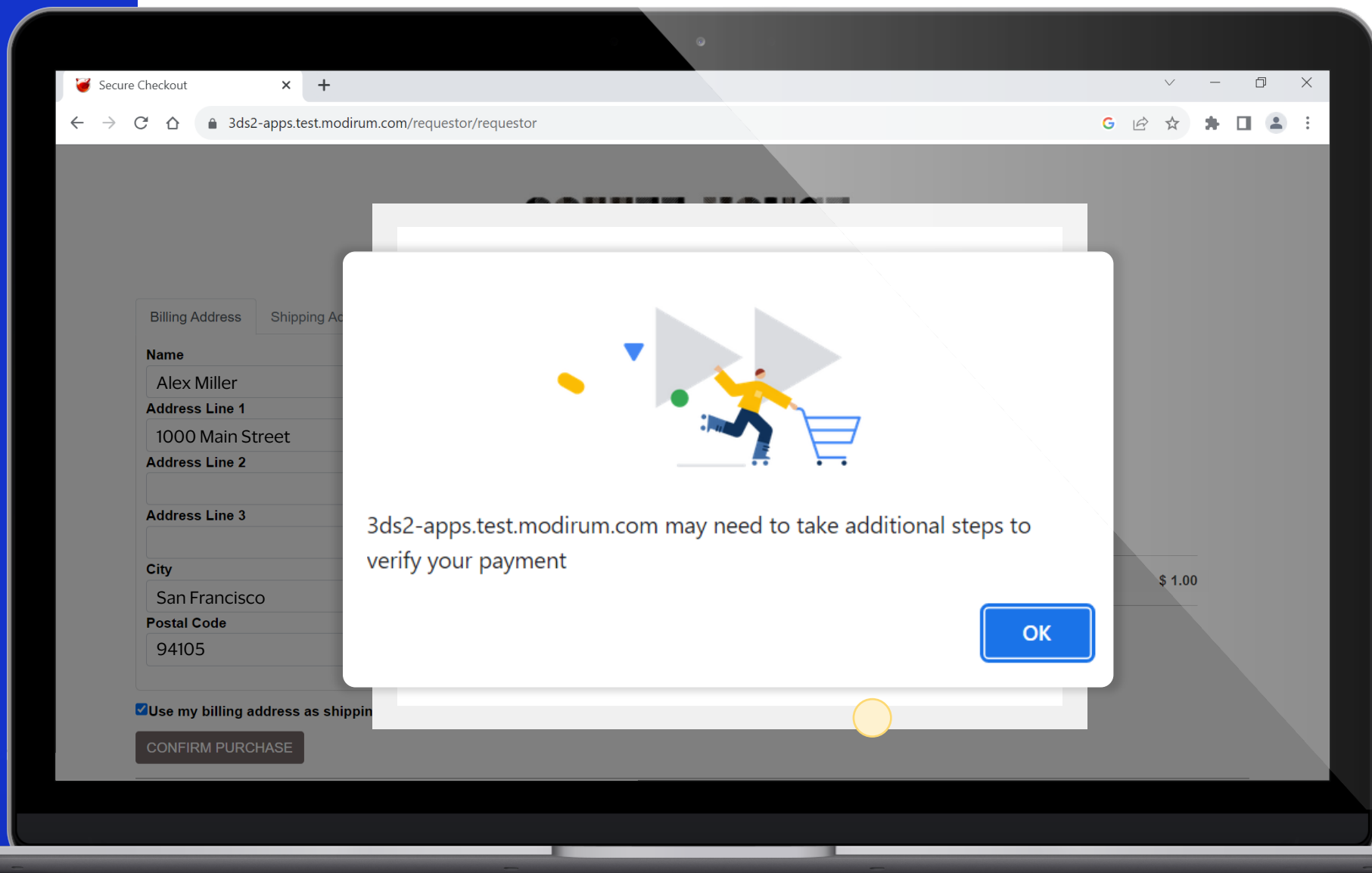
EMV 3DS is initiated

Behind the scenes, an enhanced data exchange occurs.

Authentication Required

The shopper will need to take an extra authentication step to get the transaction authorized.

SPC as the challenge method

SPC authentication starts through the mobile device.

38
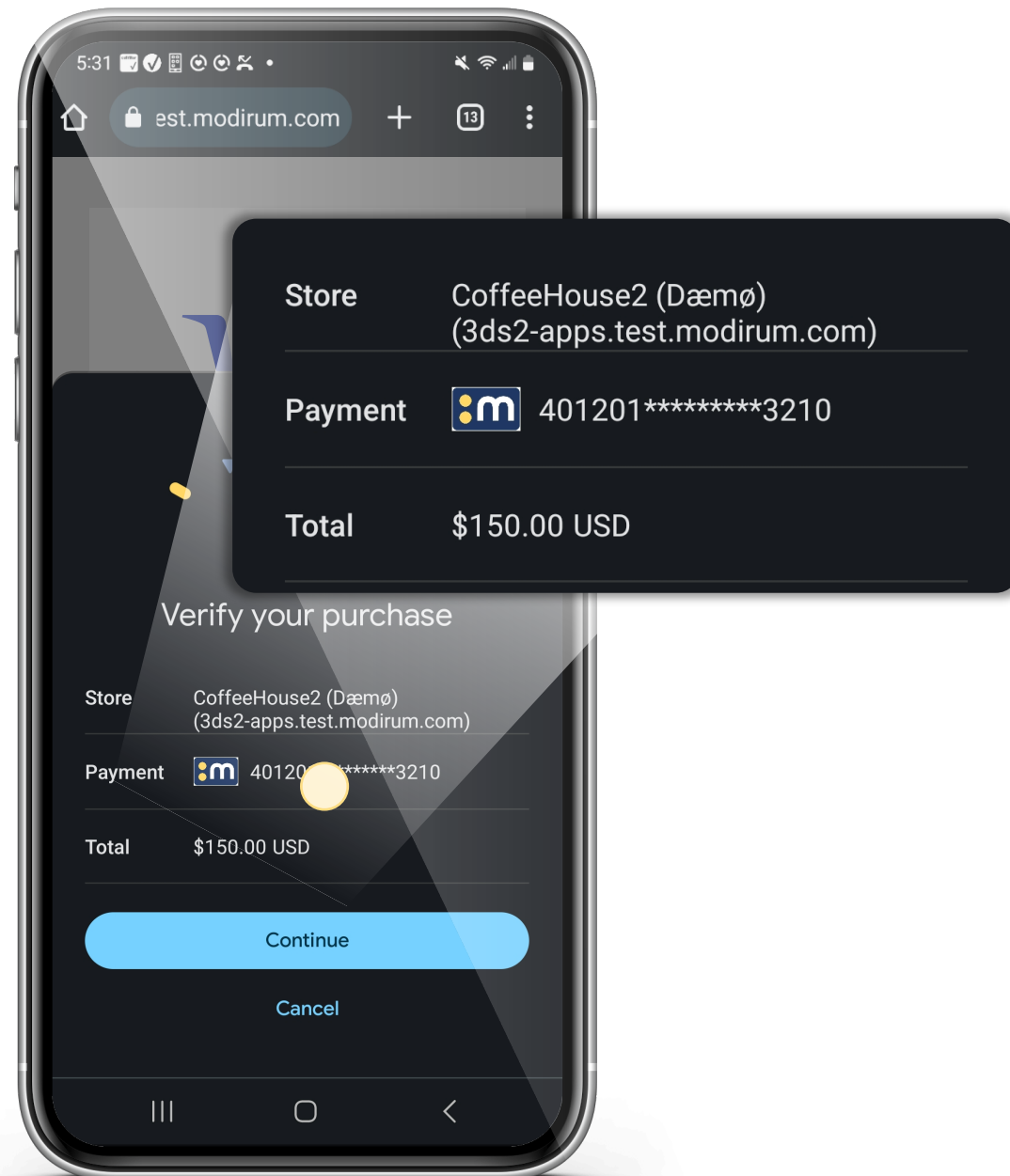
Biometric authentication

A successful biometric authentication is done via SPC.

Transaction complete

Transaction is now authenticated and order has been submitted.
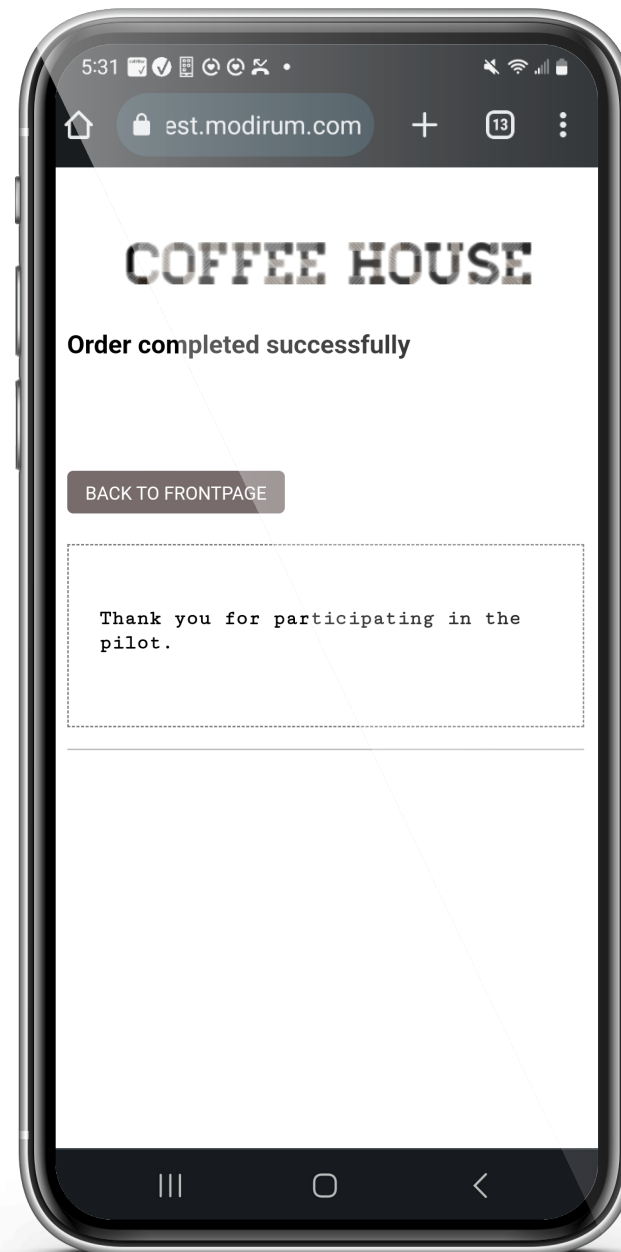
Online Shopping begins...

Now we'll do an eCommerce transaction with a desktop.
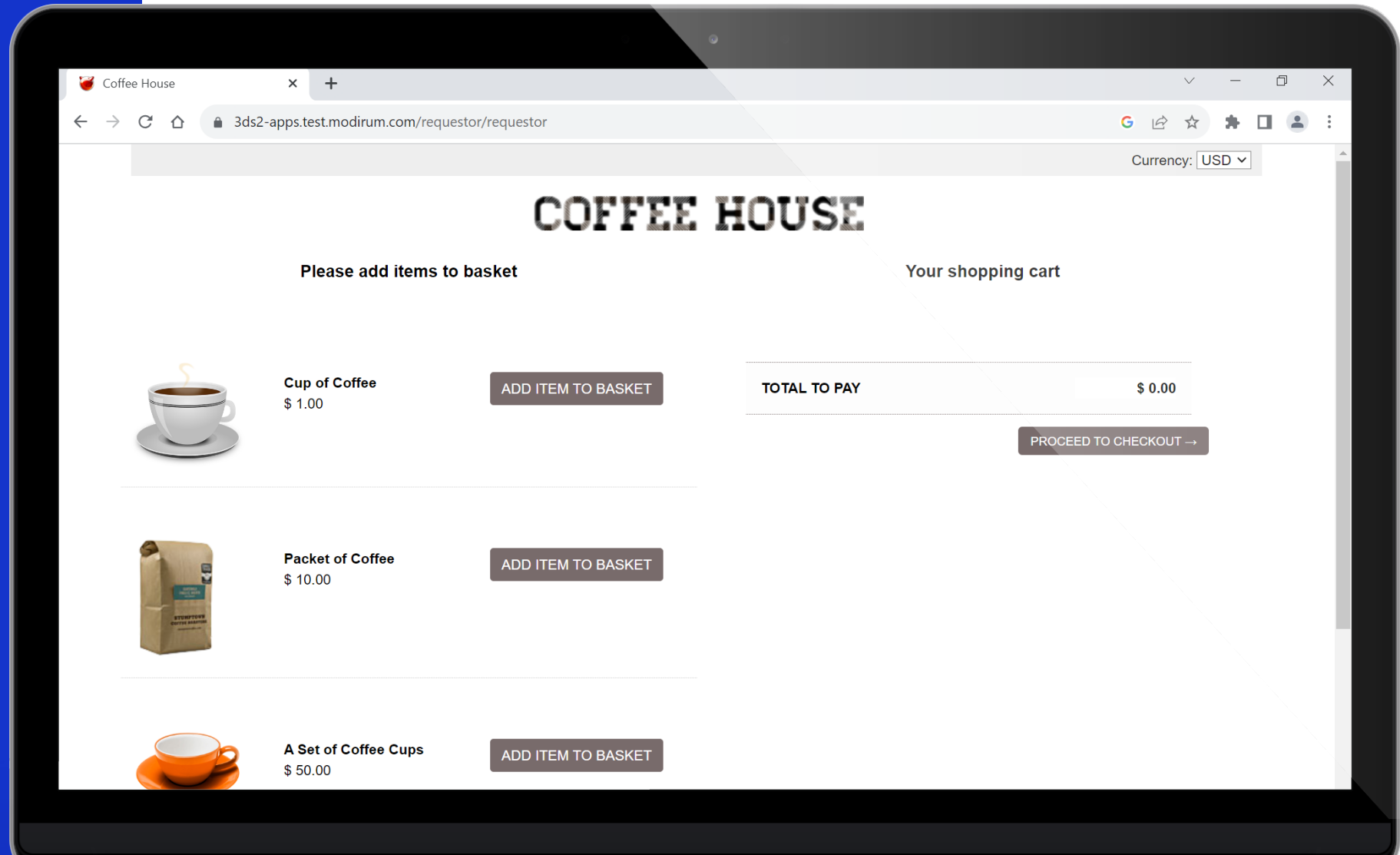
Looking for an item to purchase

In this example, I plan to buy a cup of coffee.
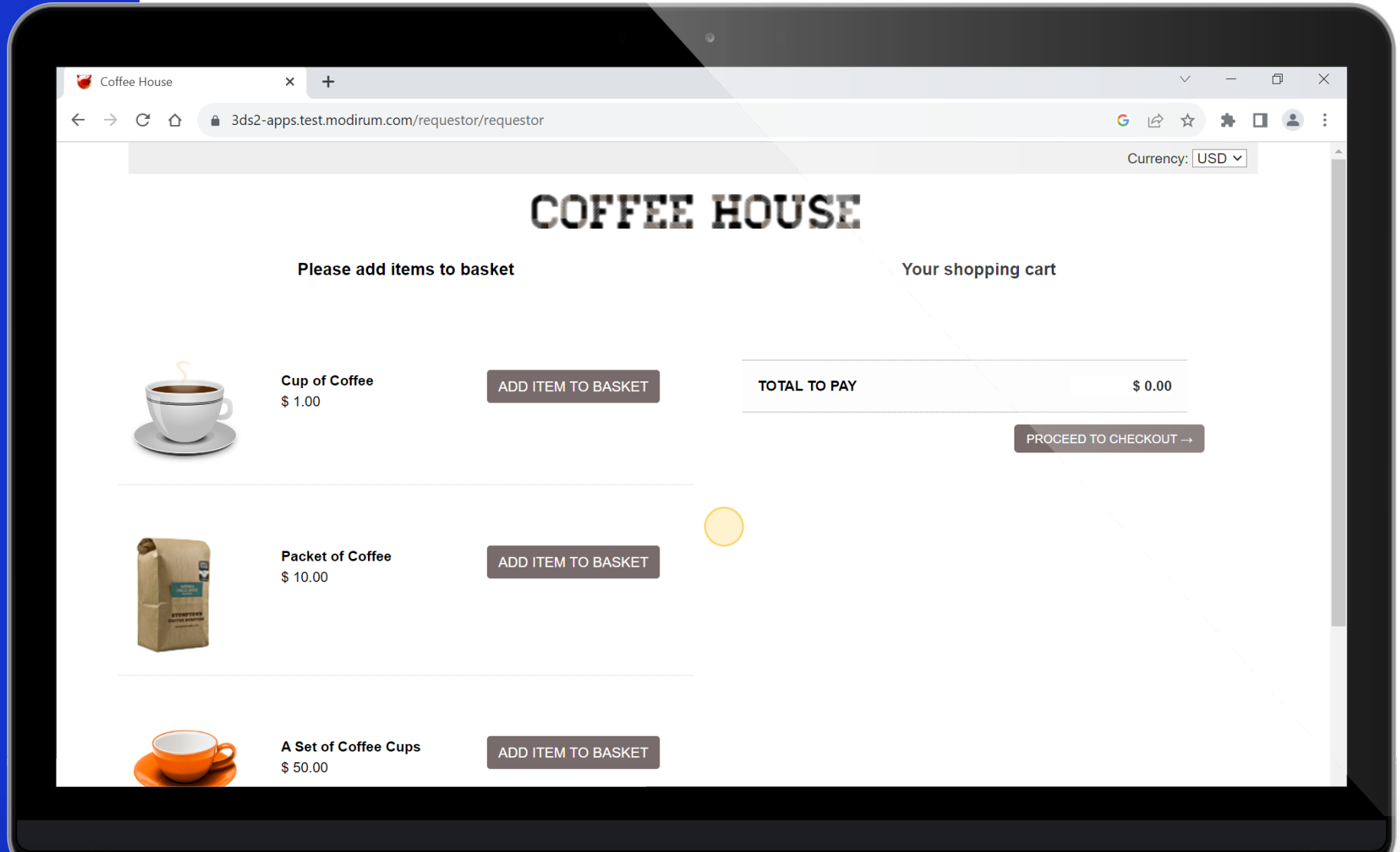
Starting the checkout process

Card details are entered into the payment screen.

Initiating the purchase

After contact, billing, and shipping address is entered, the shopper clicks the Purchase button.

EMV 3DS is initiated

Behind the scenes, an enhanced data exchange occurs.

Authentication Required

The shopper will need to take an extra authentication step to get the transaction authorized.
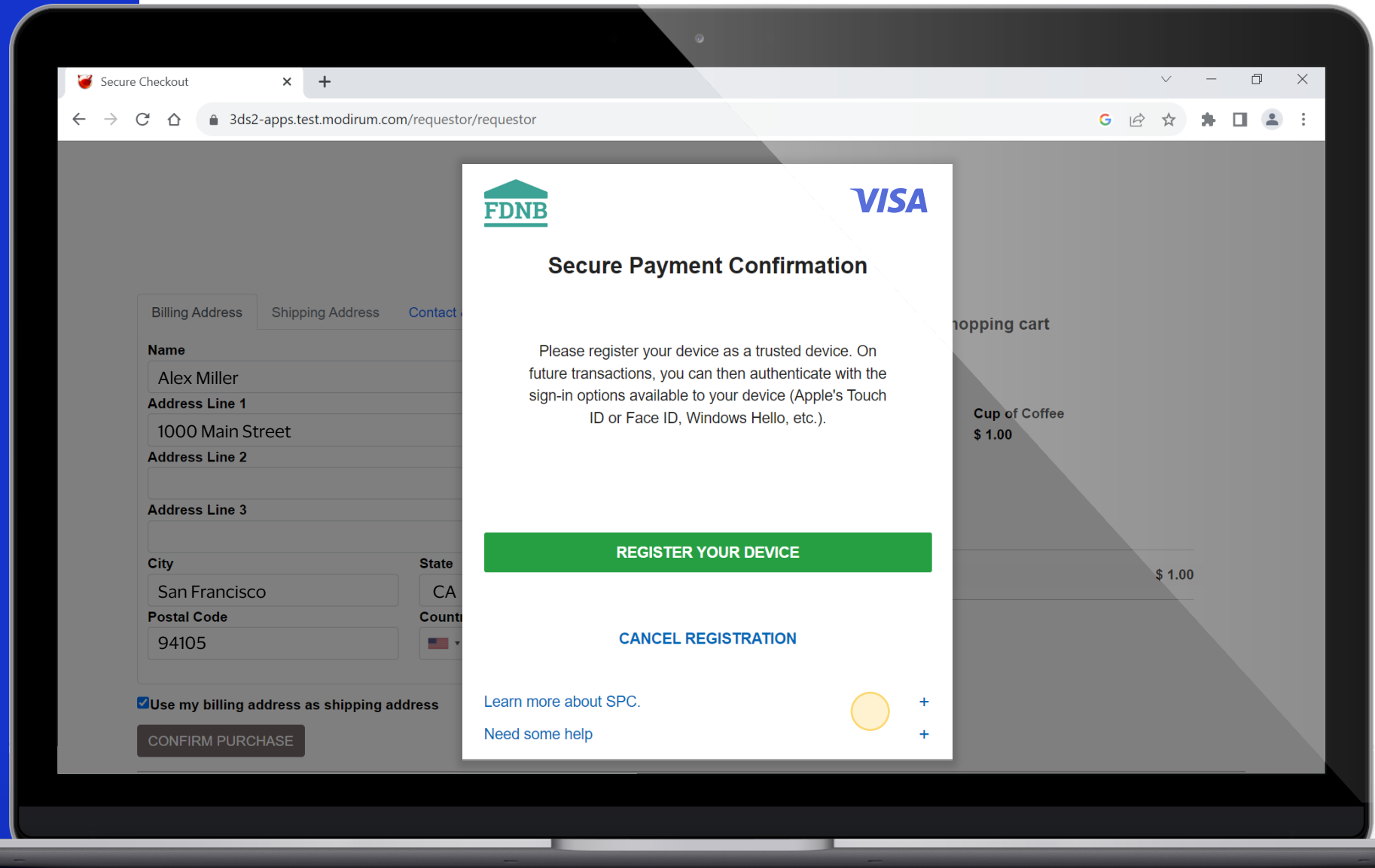
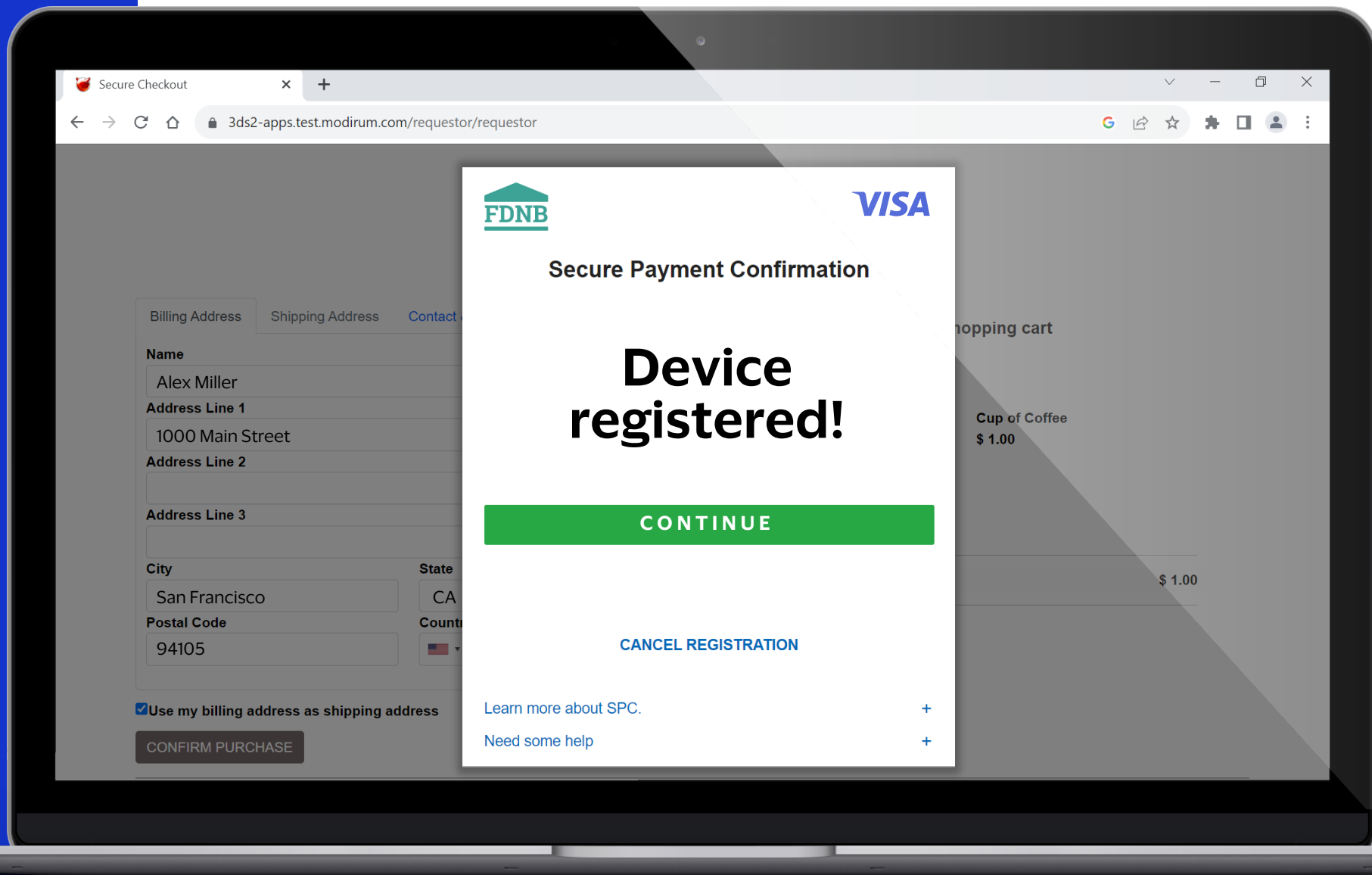# OTP Verification

Shopper is verified by OTP
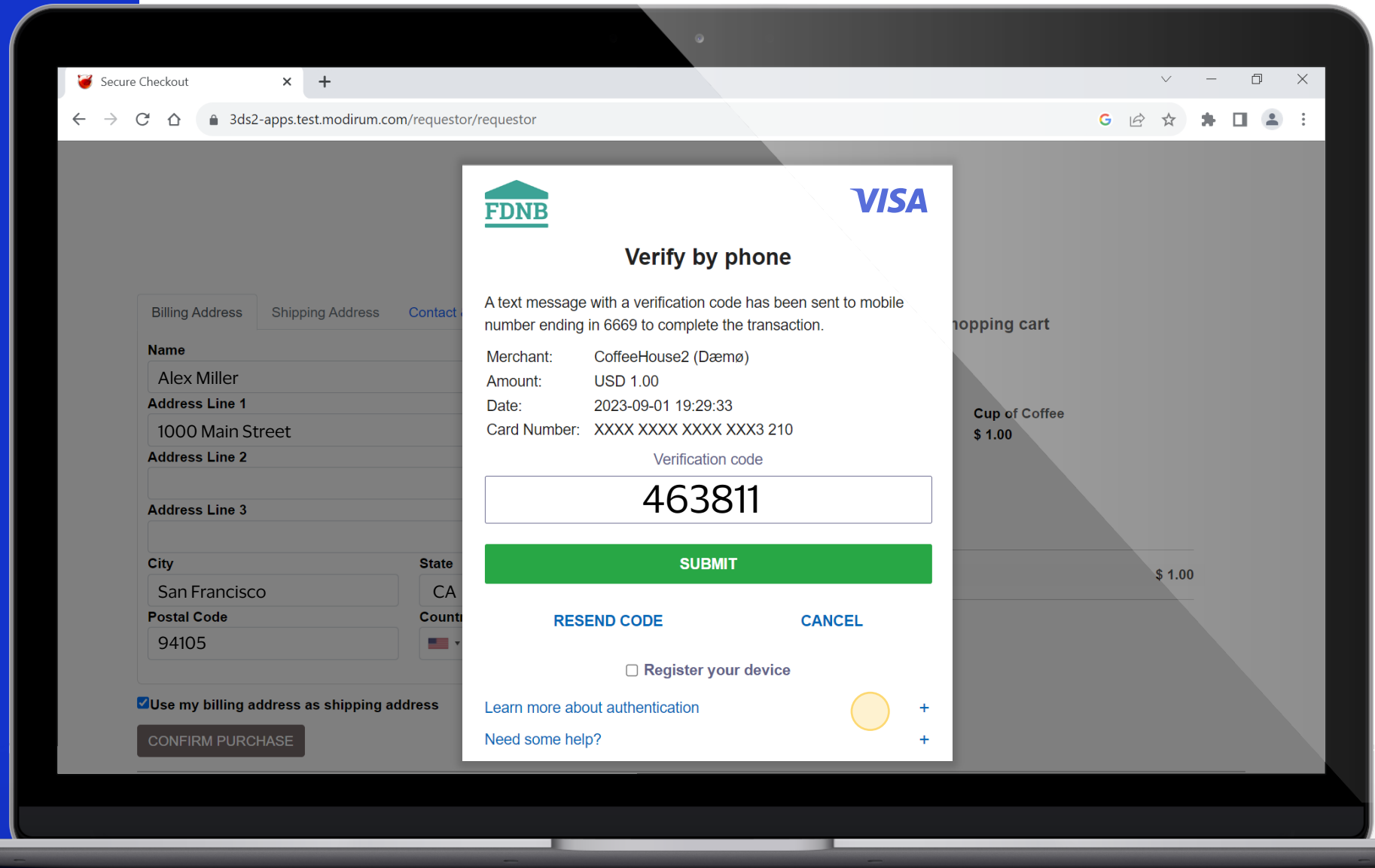
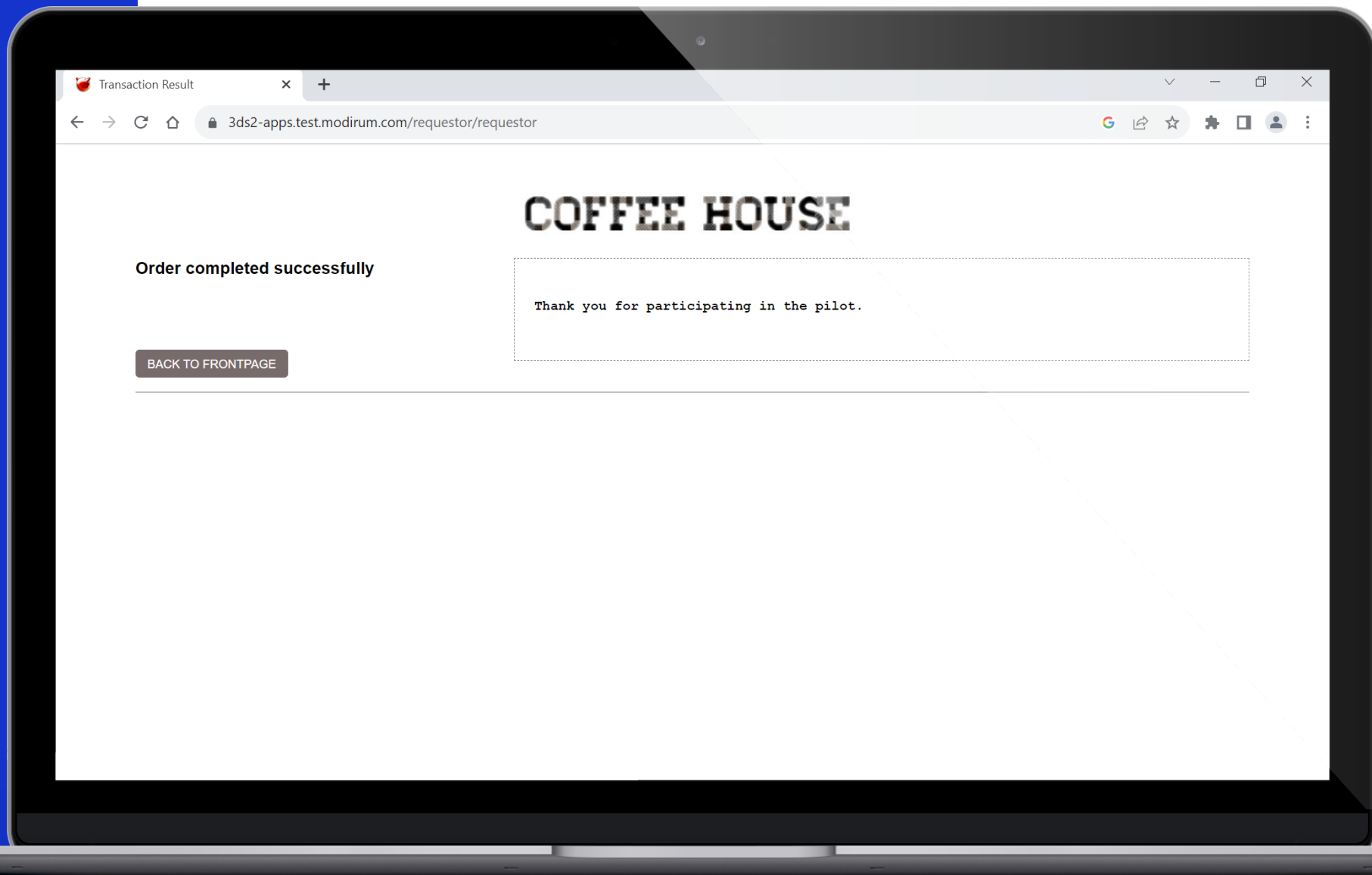# Device registration

SPC device registration is initiated.

Device is now registered

Transaction complete

Transaction is now authorized and SPC is now in place on the device.

Thank you