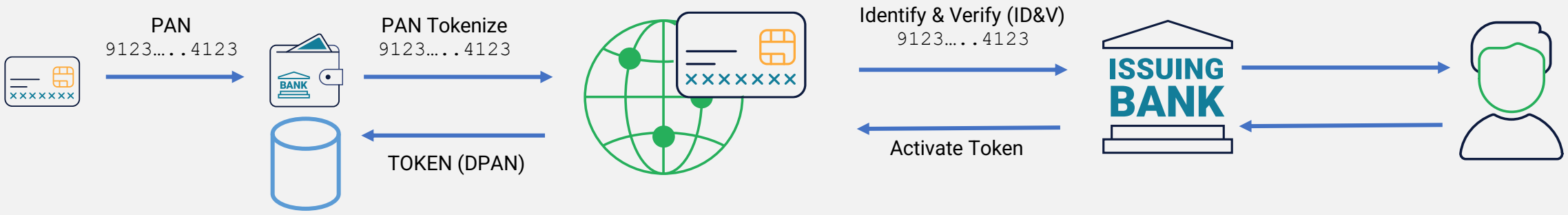
Issuing payment tokens

A possible next feature for SPC…

What is card tokenization?

- Tokenization's purpose is to reduce the impact of card data theft (PAN/Expiry Date/CVV)
- Actual Card PANs are replaced with form-preserving card tokens (DPAN)
  - Each token has a public-private keypair linked to it which is used during transaction authorization
- Card tokens are specific to a merchant (card on file) or on-device-wallet
  - These can only be used for transactions from that merchant or on-device-wallet
- Tokenization allows for merchant-based transaction authentication



How many of these tokens are being issued?

Since launching VTS in 2014, Visa said it had issued 1 billion tokens by 2020, after which growth accelerated to **2 billion** in 2021 before doubling **this year** (2022).

Visa, August 2022

Visa Token Services Surpasses **5 Billion Token** Milestone

Visa, February 2023

PayPal Braintree Reaches One Billion Cards Tokenized Globally

Paypal, August 2023

The following token-types dominate

Third party wallets
(Hardware)

Token PAN and key-pair is stored in hardware.
Token may be used across multiple merchants

In-store and eCommerce payments allowed.

Issued by adding card to the wallet

eCommerce tokens

Token stored on file, keypair in the cloud
Consumer wants to add a card to their digital wallet.

Typically issued during eCommerce transaction
('enable faster payments next time')
Could also be stand-alone issuance

Everyone is using tokens for returning cardholders…

eCommerce Tokenization

Payment service providers*

stripe
adyen
worldpay from FIS
Alipay

Large eCommerce providers *

Microsoft
NETFLIX
amazon.com
Expedia

Third party wallets *(Hardware)*

Payment service providers *

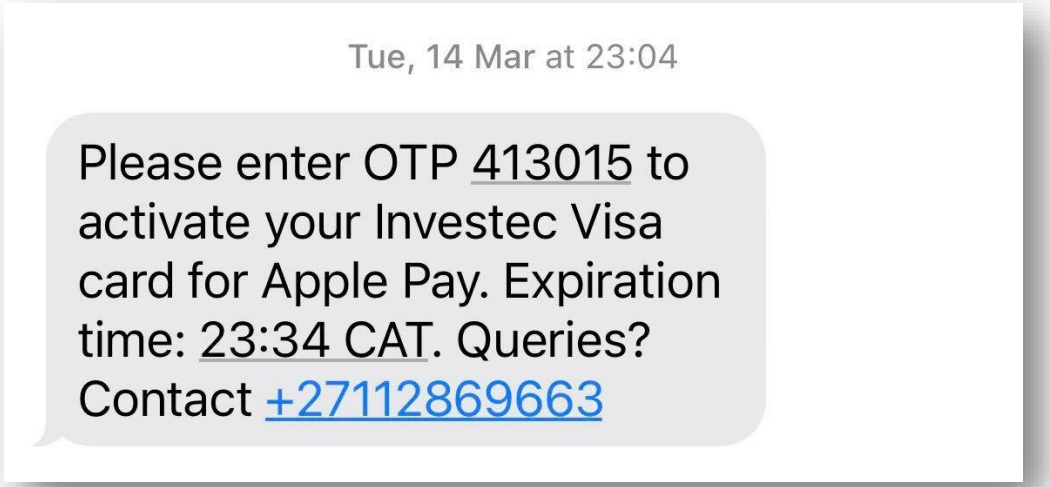
Pay
Google Pay
GARMIN PAY
Pay SAMSUNG pay
fitbit pay

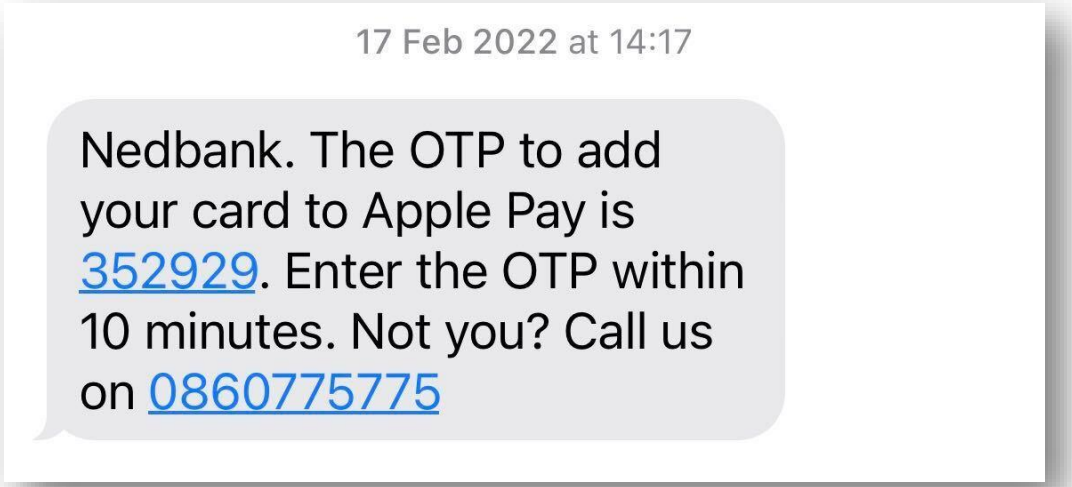
Secure Remote Commerce

DISCOVER NETWORK
AMERICAN EXPRESS
VISA
MasterCard

* Examples only

How is token provisioning protected?

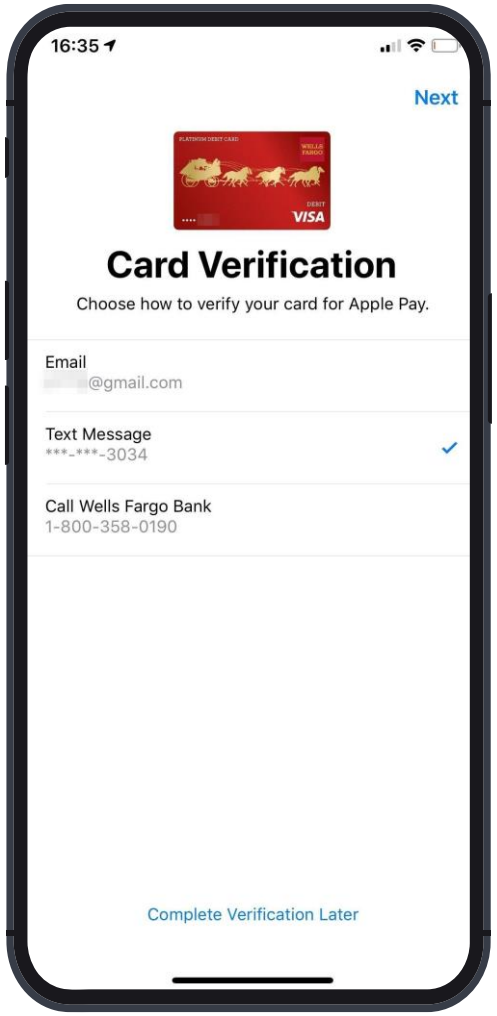


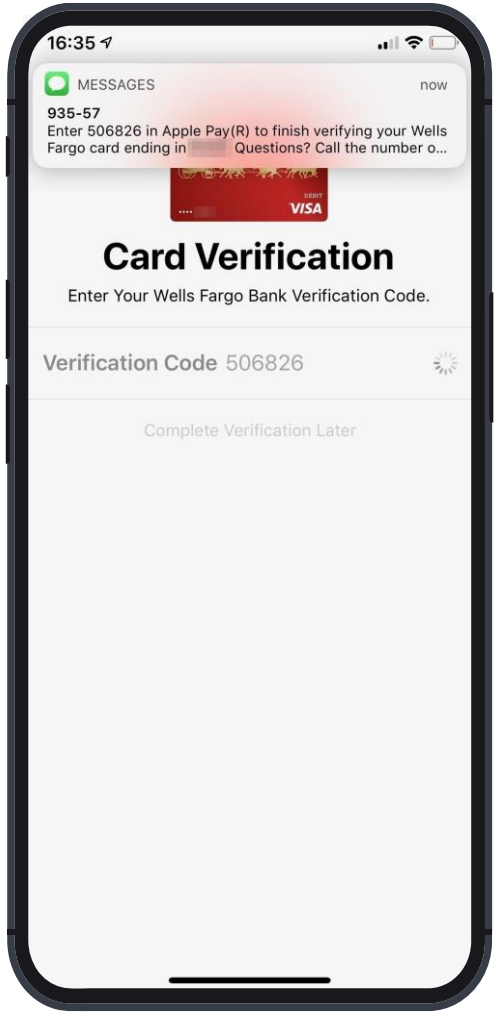


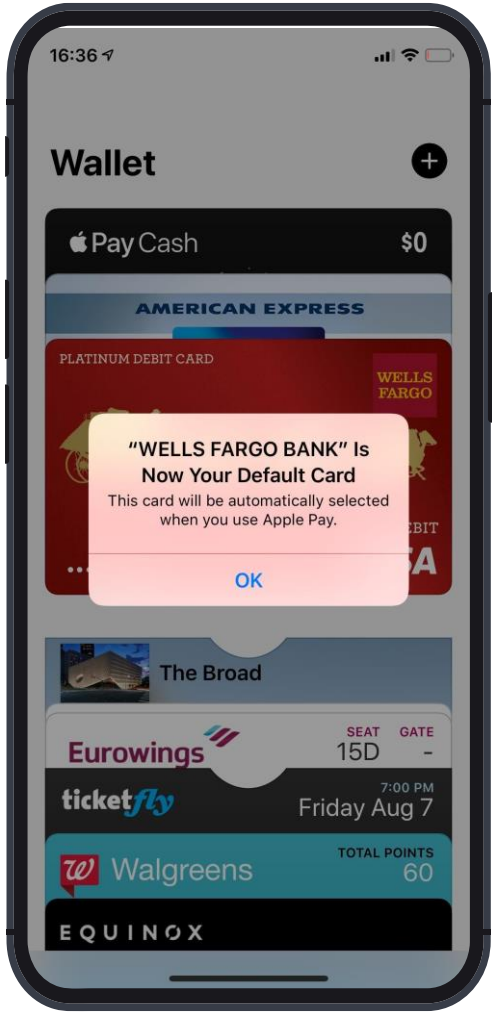
Most banks are still using SMS OTP to authenticate!

There are alternatives such as outbound call center call and bank app authentication does exist, the UX is just gets messy…

And the journey in Apple Pay

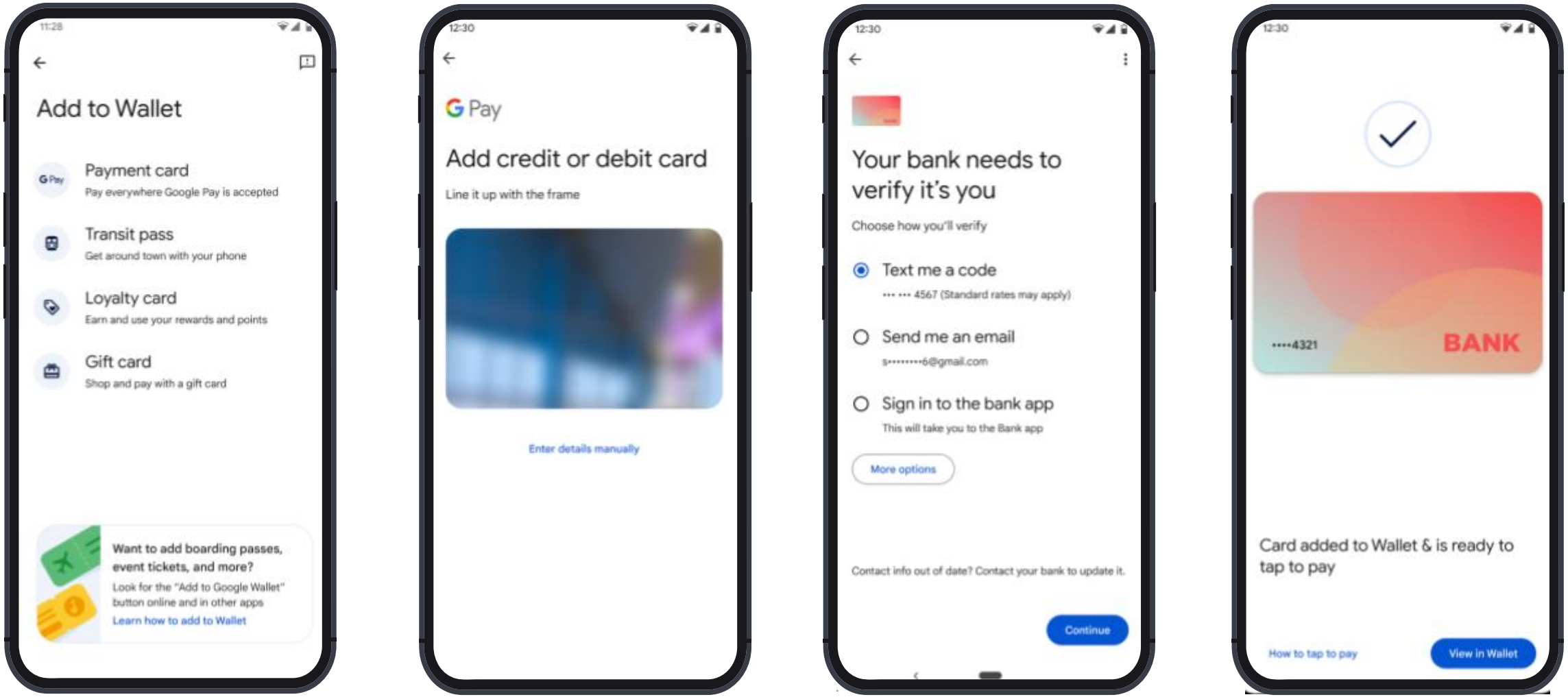






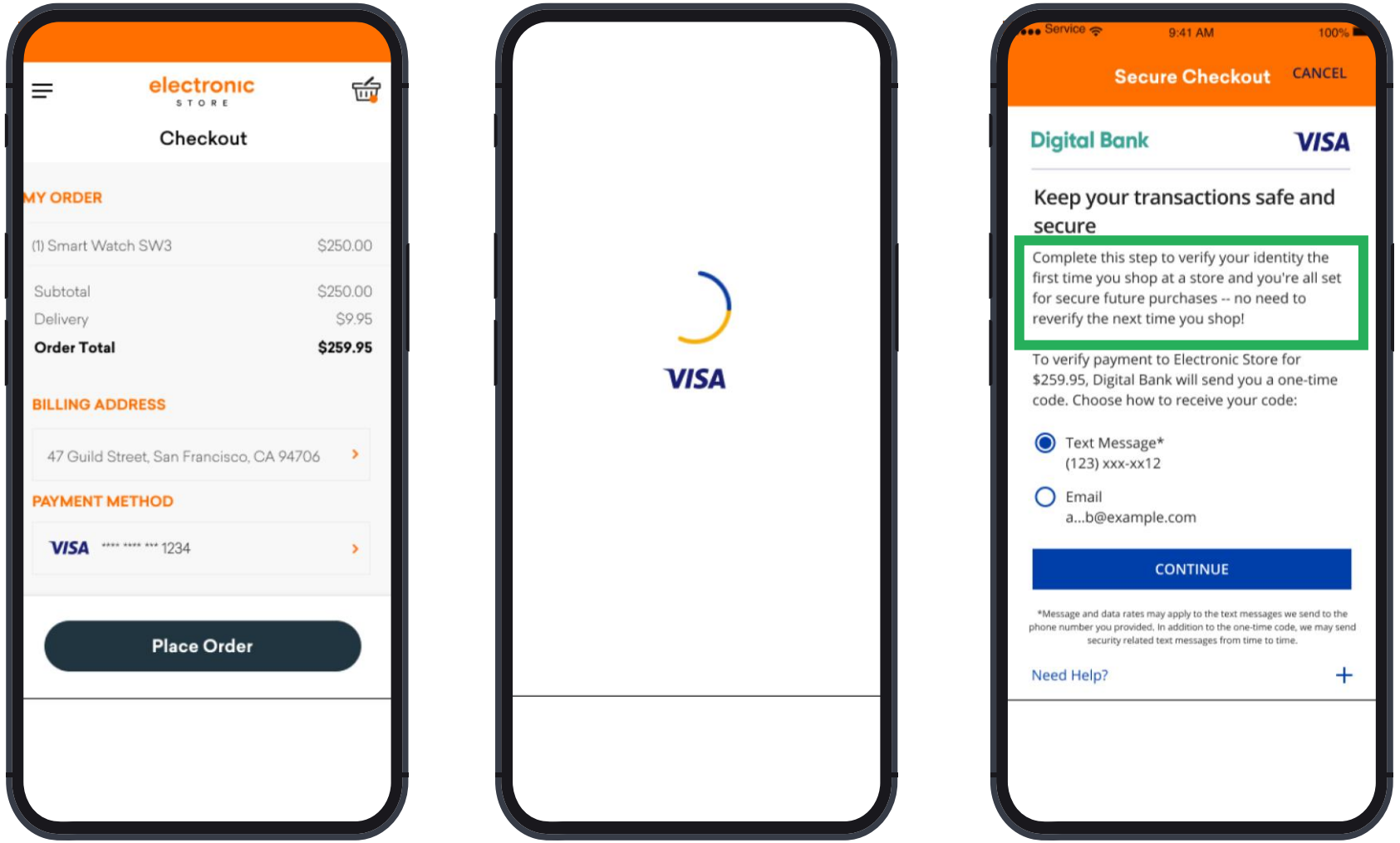
https://ios.gadgethacks.com/how-to/add-remove-debit-credit-cards-for-apple-pay-your-iphone-0197234/

Third party wallet flow



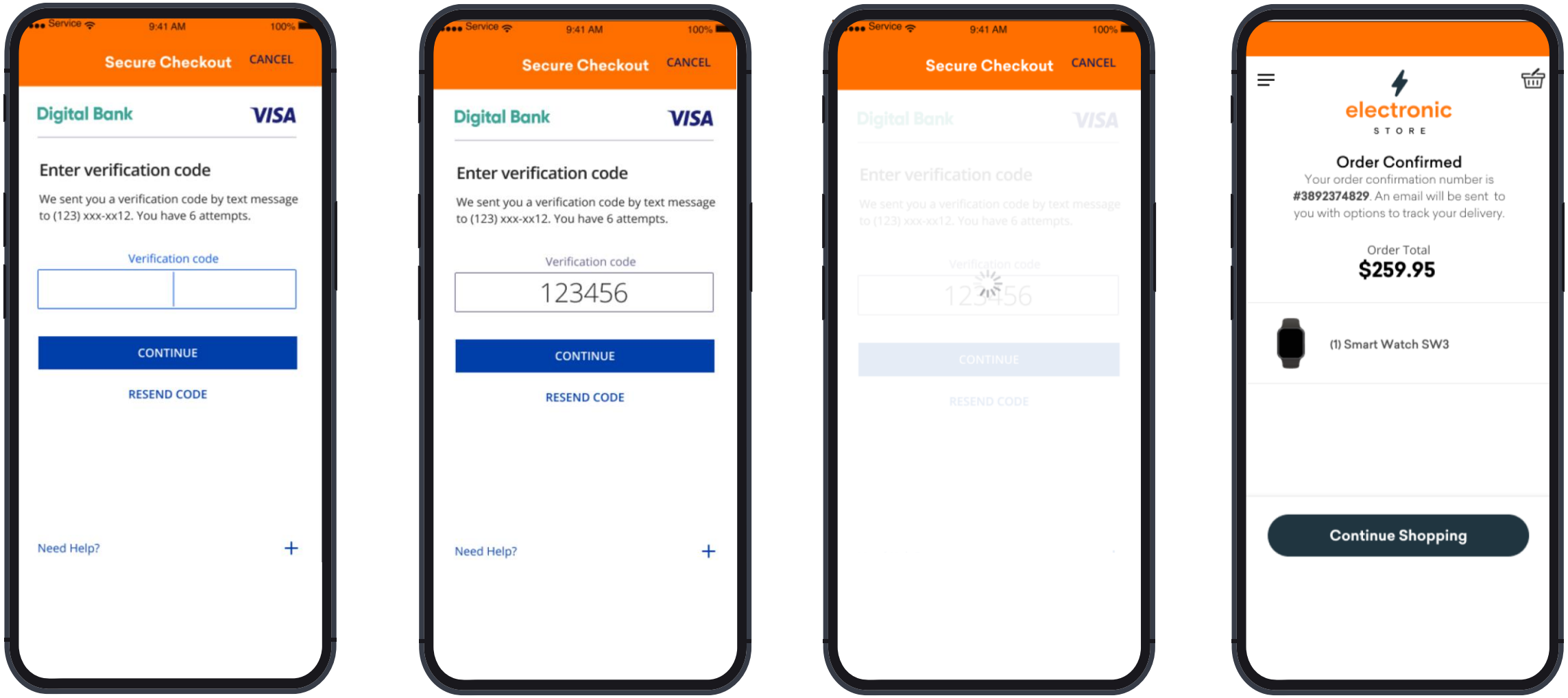
https://developers.google.com/pay/issuers/tsp-integration/gpay-flows

The ID&V process during a payment…

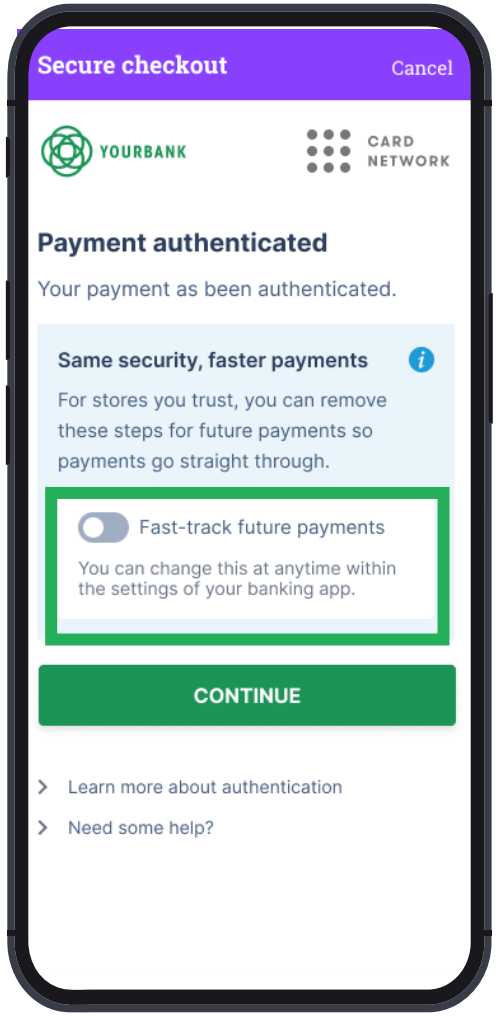


https://developer.visa.com/pages/visa-3d-secure/DigitalAuthenticationFramework

The ID&V process



3D Secure 2


Secure checkout
Cancel
YOURBANK
CARD NETWORK
Payment authenticated
Your payment as been authenticated.
Same security, faster payments
For stores you trust, you can remove these steps for future payments so payments go straight through.
Fast-track future payments
You can change this at anytime within the settings of your banking app.
CONTINUE
Learn more about authentication
Need some help?

The card token provisioning is a high risk activity and an important part of enabling secure payments

Use SPC to confirm the issuing of a card token

The potential roles of SPC in eCommerce

Provisioning

Issue a new card token into a wallet.
The wallet is responsible to protect the token.

Issuance during eCommerce

Merchant may bind their own credential for consent.

Stand-alone issuance

Transaction

Use a card token to perform a transaction.

SPC can be used to confirm payment

Traditionally this uses an ***Issuer credential***
SPC allows this to be used in the Merchant domain

Tokenization and Delegated Auth allows a Merchant credential to be used

The issuer is informed but may/should not challenge.

This is enabled via two protocols:
3D Secure OR card association tokenization API

Data Element/ Field Name	Description	Source	Length/Format/Values	Device Channel	Message Category	Message Inclusion	Conditional Inclusion
3DS Requestor Authentication Indicator	Indicates the type of Authentication request.	3DS Server	Length: 2 characters JSON Data Type: String Values accepted: • 01 = Payment transaction • 02 = Recurring transaction	01-APP 02-BRW	01-PA 02-NPA	AReq = R	
Field Name: `threeDSRequestorAuthenticationInd`	This data element provides additional information to the ACS to determine the best approach for handling an authentication request.		• 03 = Instalment transaction • 04 = Add card • 05 = Maintain card • 06 = Cardholder verification as part of EMV token ID&V • 07 = Billing Agreement • 08 = Split shipment • 09 = Delayed shipment • 10 = Split payment • 11–79 = Reserved for EMVCo future use (values invalid until defined by EMVCo) • 80–99 = Reserved for DS use				

Tokenization aims to reduce friction at checkout

Visa and Mastercard have both introduced tokenization programs to
reduce friction by
shifting the burden of **authentication** from issuers **to merchants**

Visa ***Digital Authentication Framework (DAF)***

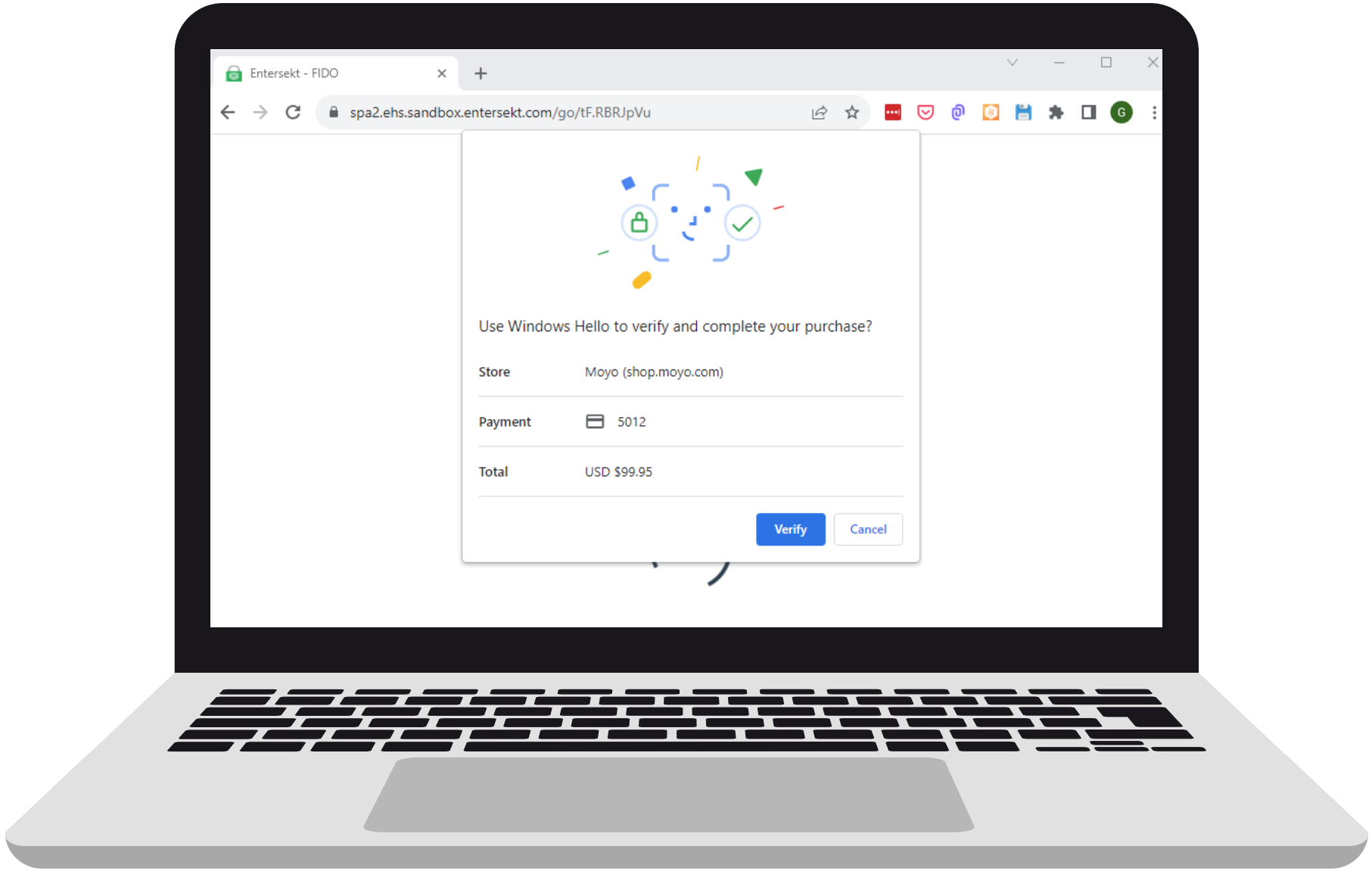
- Issuers are not allowed to request a step-up or challenge on subsequent authentication requests from the same merchant, customer, and payment account that meet the DAF requirements
- Issuers are liable for fraud on authenticated transactions that meet DAF requirements.

Mastercard ***Token Authentication Framework (TAF)***

- Merchants authenticating remote commerce token transactions with an approved multi-factor authentication (MFA) method will be liable for those transactions

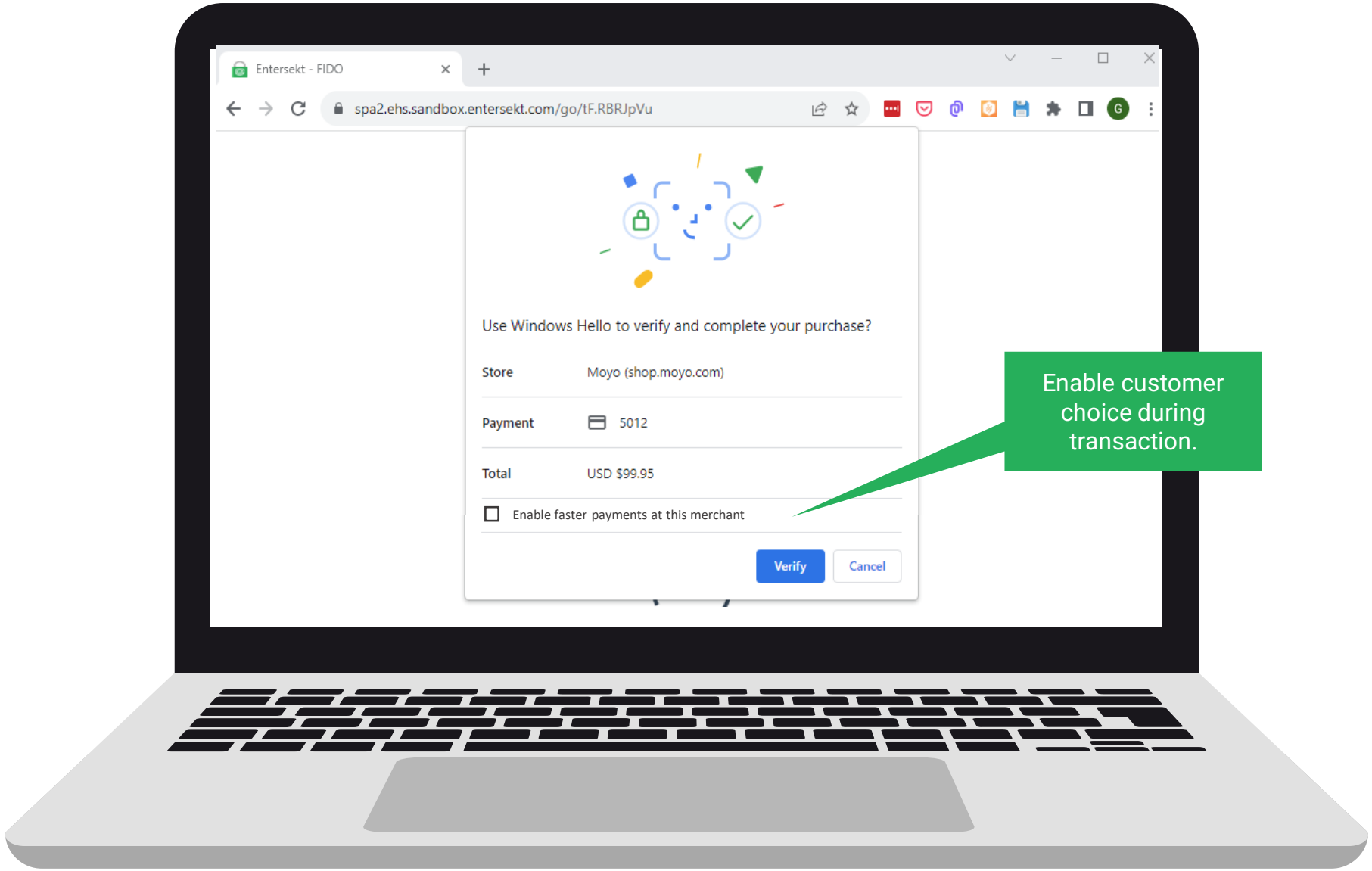
https://www.entersekt.com/knowledge-hub/blog/tpost/1u9h7tu1b1-daf-and-taf-what-changes-merchants-and-i

Standard SPC only caters for the payment

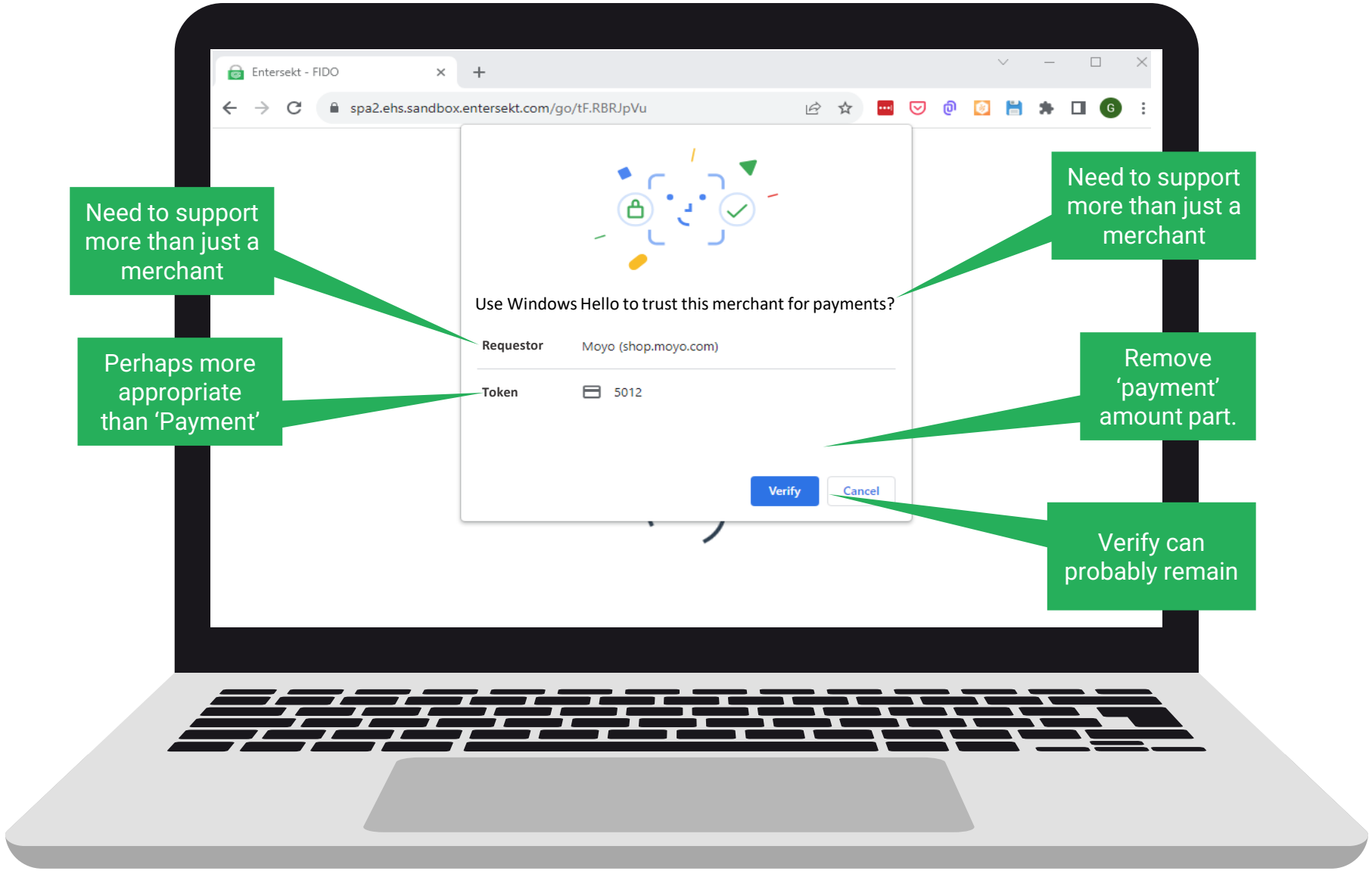


17

Proposal: enable provision during shopping



Suggestion: Enable provision without shopping



Discussion time

Thank you…