entersekt

Payment Fraud Patterns

Entersekt

ERHARD BRAND

2022/09/15

Important notice - confidential information

The information in this document contains confidential information that is the property of Entersekt and is legally privileged. Access to the contents of this document is subject to the signing of a non-disclosure agreement with Entersekt. Access to this document by anyone without a signed NDA in place with Entersekt is unauthorized. If you are not the intended recipient, or do not comply with the above mentioned condition, any disclosure, copying, distribution or any action taken or omitted in reliance on it, is prohibited and may be unlawful.

No part of the contents may be used, copied, disclosed or conveyed in whole or in part to any party, in any matter whatsoever without prior written permission from Entersekt.

All copyright and intellectual property herein vests in Entersekt.

Permitted distribution: NDA-Only

Who we **are.**

Backed by: AKKR, Endeavor Catalyst, RMI

Founded in **2010**

10x faster authentication than SMS OTP

>78 million enrolled users

1.1 billion+ sessions secured every month

170+ employees globally

85+ Banking & FI clients

99.99% uptime

>22% higher 3DS transaction success rate than industry average

A few of our customers

Capitec Bank, Plus Card, Brex, Investec, mastercard, Standard Bank, Cash App, 1st Bank

A few of our partners

NuData Security mastercard, Mambu, onewelcome, netcetera, onfido, Q2

Certifications

ISO/IEC 27001:2013 Information Security Certified by Sancert, fido Certified FIDO2, EMVCo, Verified by VISA, mastercard ID Check, American Express SafeKey, Discover, Diners Club International, ProtectBuy

entersekt

The industry

The industry

- **Payment fraud is a massive problem, growing every year**
- **Card-Not-Present transactions are more vulnerable, as it's difficult to identify the customer**
- **Anti-fraud workflows are tough to build**
- **You also have to weigh the measures you put in place up against the customer experience:**
  - Too little and you run the risk of your customer being defrauded
  - Too many and you run the risk of transaction abandonment

The impact of **poor payment authentication**

Poorly implemented fraud prevention tools have a negative business impact:

52%
of orders declined for fraud were good orders to fulfill

62%
of cardholders will abandon a declined card

Sub-optimal user experiences regularly result in abandonment

65%
of customers abandoned carts due to friction

>$100 billion
in sales foregone due to friction at checkout

Bad checkout journeys result in abandonment, which costs the customer and the bank.

Sources: Ethoca Research; Solving the CNP False Decline Puzzle; Visa; Ekata

Authentication experiences can be better

Secure and seamless
multi-factor-authentication
enabling
passwordless experiences.

Authentication which
protects your customers
and exceeds
regulatory requirements.

Contextual authentication
selecting the optimal
customer journey

entersekt

Our position as Auth Provider & ACS

Our position as Auth Provider & ACS

- **Clients use us for:**
  - Front-door auth
  - Step-up auth
  - Auth provider for their existing ACS flows
  - Or our own ACS
- **Entersekt has a unique vantage point:**
  - We see the customer during login at their bank
  - Also see them during an online purchase when performing a challenge during a 3DS flow

- **Our authentication solutions includes:**
  - App / SDK: 2FA OOB Push Auth (including biometrics)
  - Web: FIDO Auth (with SPC)
  - Web: Browser ID to identify returning browser's
  - Web: User behavioral biometrics (Partner)
  - Phone: USSD, SMS OTP, Voice Auth (Fallback)

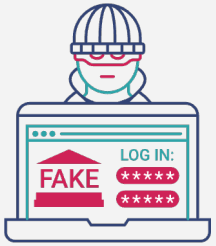
Source: UNCTAD: Estimates of global e-commerce, 2019: https://unctad.org/system/files/official-document/tn_unctad_ict4d18_en.pdf

entersekt

Identified fraud patterns

Identified fraud patterns

- **Payment fraud is an entire value chain**
  - Stealing of credit card numbers
  - Password leaks / breaches
  - Attempt small purchases with credit card numbers to identify valid cards
  - Attempt banking portal login's using stolen credentials to identify valid users
  - Attempt banking portal login's using stolen credentials to extract PII
- **Once data has been filtered the fraudster has access to a complete profile**
  - Valid PAN
  - Valid username & password
  - Valid email address & phone number
- **Fraudster has options**
  - Use acquired info to purchase goods
  - Use acquired info to perform social engineering to perform account takeover -> push payments
  - Sell it to the highest bidder



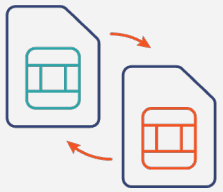
Identified fraud patterns

- **Account Takeover: Phishing (Common)**
  - Elements required:
    - Customer's e-mail address, phone number

  - How it's done:
    - Fraudster creates website that looks exactly like the bank / FI's
    - Sends customer an e-mail or SMS containing link: "Please verify your details as part of our security audit" / "Your account is at risk, verify your details now"
    - Asks the user to provide username & password on the phishing website
    - Logs in to customer's account, transfers money (push payment, often no challenge required) to mule account
  - How it's mitigated:
    - Require customers to enable 2FA (OOB to mobile app, FIDO) on sensitive transactions (a new beneficiary)
    - Run campaign to educate customers to not click SMS / e-mail links

Identified fraud patterns

- **Account Takeover: SIM Swap (Common)**



  - Elements required:
    - Customer's Credit Card number
    - Customer's PII (Name, telephone number, home address)

  - How it's done:
    - Fraudster calls mobile network operator (MNO) and requests sim swap, or has internal contact
    - Once sim swapped, SMS OTP codes will be delivered to fraudster
    - Perform fraudulent transaction, using OTP to verify purchase

  - How it's mitigated:
    - Request "Sim Info" from MNO for specified MSISDN
    - "Sim Info" contains "Sim age"
    - If Sim age < 2 days, flag transaction to perform step-up auth / call customer or outright decline
    - Immediate impact on % of fraud events at multiple customers we have worked with

Identified fraud patterns

- **Account Takeover: Social Engineering (Common)**
  - Elements required:
    - Customer's bank details
    - Customer's PII - the more you have, the more at ease the customer will be
    - Existing auth mechanism should use generic messaging: "Are you performing a sensitive action? Yes / No"
  - How it's done:
    - Fraudster calls customer, posing as bank employee
    - Tells customer they will perform security check, can expect a challenge message and should approve it
    - Logs in to customer's bank account, transfers money to mule account
  - How it's mitigated:
    - Implement behavioral biometrics
    - Update challenge to use specific messaging. Should be short & concise. Order actually makes a difference: "Do you want to transfer $1000 from Savings Account?" Vs "Transfer $1000 from Savings?"

Identified fraud patterns

- **Chargeback Fraud (Common in markets where 3DS are not used)**
  - Elements required:
    - Customer's Credit Card number
    - Customer's PII (Name, telephone number, home address)
    - Bank / FI should not use purchase confirmation messages post-purchase (SMS, Push Notifications)

  - How it's done:
    - Buy goods on a legitimate website using stolen credit card details
    - Once goods have been received, fraudster applies for refund from merchant
    - Customer's balance remains neutral, so they don't notice. Doesn't scrutinize CC statements
    - Even if the client does realize something is wrong, they will request a refund from their bank, fraudster keeps the goods
  - How it's mitigated:
    - Implement 3DS challenge flow and improved confirmation messaging post-transactions

Identified fraud patterns

- **Triangulation Fraud (less common)**
  - Elements required:
    - Customer's PII

  - How it's done:
    - Fraudster sets up fake storefront offering items at discounted prices
    - Customer places order using their credit card
    - Fraudster orders the requested item from an online retailer, ships it to the customer
    - Customer is happy with their "good deal"
    - Fraudster now has customer's card details for future use
    - Customer can also pay using Bitcoin, fraudster use stolen CC details to order goods
  - How it's mitigated:
    - Implement 3DS challenge flow
    - Use descriptive messaging during 3DS challenge during online purchases

Identified fraud patterns

- **So, what does this mean?**
  - Covid-19 fueled a rise in online transactions: April 2022 US retailers YoY online growth was up by 68%[1]
  - Account Takeover is a problem, up by 300% from 2019 to 2021[2]
  - Merchant's need to enable the 3DS flow, preferably using a challenge/response mechanism where customers are required to authenticate in real time
  - Card tokenization defeats numerous of the fraud attack vectors, where tokens are one-time-use
  - A lot of these attacks could be mitigated if we were to identify returning browsers
  - Communication during / after online payment flows should be descriptive, yet concise

[1] Tala, Global Data At Risk: State of the Web Report, 2022
[2] Sift & Card Not Present: Evolving Account Security for the Passwordless future, 2022.

entersekt

Zooming in on the browser

Zooming in on the browser

- Card sniffing / skimming attacks / Magecart group
- Effectively used XSS to insert modified JavaScript into merchant pages
- Scanned S3 buckets for write access, overwrite existing .js files with updated files containing modified JavaScript[1]
- Happened outside the organization that rely on the code, remote code being loaded
- Compromised JavaScript being executed on payment pages, stealing card data
- 17 000 domains affected
- What could help:
  - JS integrity hash being included when loading the JS
  - Strict Content-Security-Policy (CSP) rules to prevent outbound connections to unauthorized endpoints

[1]: Over 17,000 Domains Infected with Code that Steals Card Data, 2019

Zooming in on the browser

- Card testing / card cracking fraud
- JavaScript being used to test stolen credit cards for small purchases to see if the card is valid & active
- Most common form of fraud experienced by North American merchants in 2021[1]
- Will target businesses that doesn't have effective fraud prevention tools in place (e.g., 3D Secure challenge flow)
- What could help:
  - Implement 3DS challenge flow
  - Velocity checking
  - Origin IP address monitoring
  - Monitoring multiple declines on card
  - Bot detection

[1]: Changeback Gurus, Preventing Card Testing Fraud, 2022: https://www.chargebackgurus.com/blog/card-testing-fraud

Zooming in on the browser

- Overall, cross-site scripting (XSS) is still a widely used attack
- Browser fingerprints can be spoofed (spoiler for the next session)
- Other, insecure, embedded elements on the page can execute modified JavaScript
- Content-Security-Policy (CSP) rules often not implemented or lacking

Zooming in on the browser

- Ultimately, everyone needs to rely on how secure their JavaScript implementation is
- 2020 State of the Web report by Tala Security found that 92% of the evaluated websites expose data to an average of 17 domains[1]
- The average website includes content of 32 third-party JS vendors[1]

[1] Tala Security: Global Data At Risk State of the Web Report, 2021

entersekt

How to address these fraud patterns?

How to address these fraud patterns?

- If banks had access to stronger signals, especially from the browser, they could make better risk-based decisions
- Browser fingerprinting on its own isn't good enough anymore. We don't want to work against the privacy rules being put in place
- Use FIDO & SPC during 3DS flows (public-key cryptography, origin bound, app-less, widely supported)
- Are still looking for better signals to enable frictionless flow

How to address these fraud patterns?

- **Context-aware Challenges: Include the customer's geo-location**
  - If you position your Geolocation request right, customers will opt-in
  - Can be valuable to detect the geo-location in real-time
  - Mobile device geo-location more accurate than browser's
  - If a purchase was initiated in South Africa this morning and 1 hour later a purchase is made from a different continent, it's a rather good fraud signal
  - Things like VPN's etc. can influence accuracy, but when used with other data points, it could add value to risk engine

How to address these fraud patterns?

- **Offer FIDO Auth / SPC during 3DS transactions – even from within the issuer's iframe**
  - Register a user's FIDO authenticator in the 1P context while signed into the issuer's website (internet banking portal)
  - With Chrome & Safari supporting the WebAuthn APIs in a cross-origin iframe, 3DS checkout flow can take advantage of FIDO authentication during the challenge step
  - SPC can be invoked from within the iframe if supported to give an improved experience over the traditional WebAuthn dialog (Do you want to sign in to example.com?)
  - Once ready, the merchant can integrate directly to the issuer and invoke SPC from their domain (delegated)

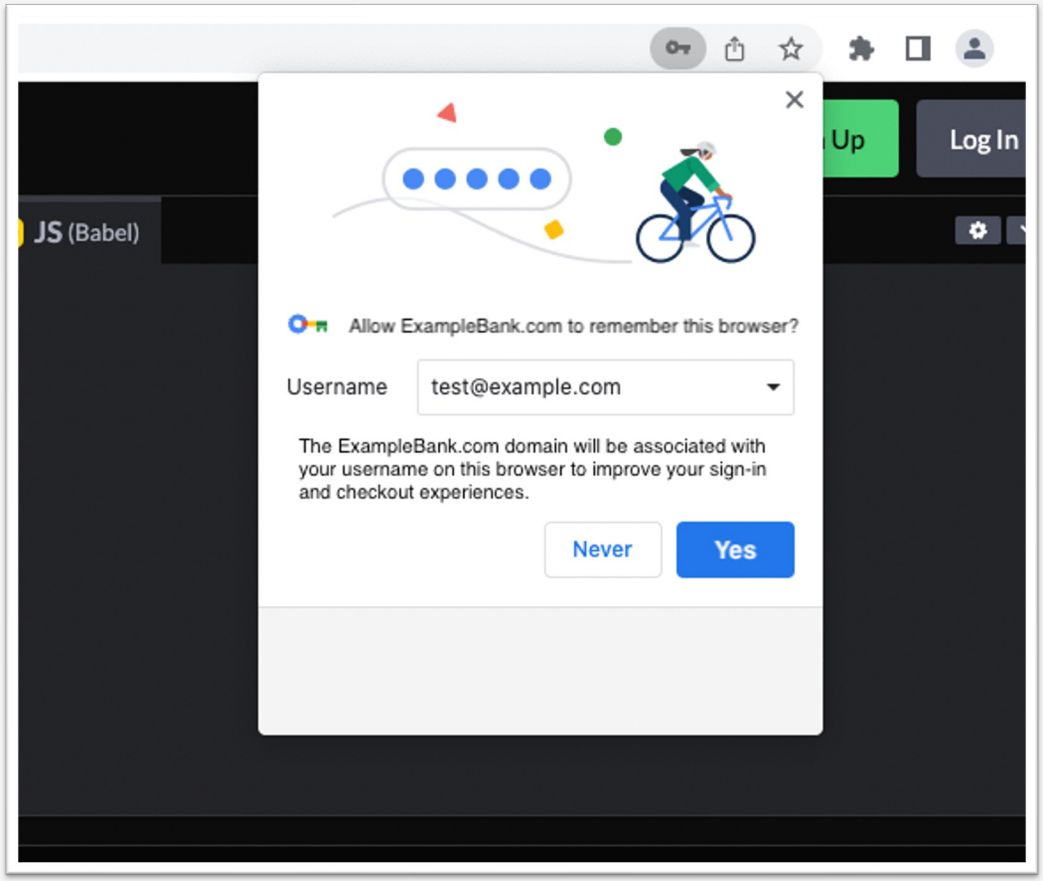
How to address these fraud patterns?

- **Browser behavioral biometrics: Use contextual data to generate a risk score for FI's to use as part of their decision-making process**
  - Detects person's familiarity and velocity with the form
  - Detects person's familiarity (or lack of) with the data (name, address)[1]
  - Multiple login attempts originating from the same endpoint
  - Modified browser detection
  - Distance travelled: Geolocation + IP checks
  - Along with other data points feeding into risk engine

[1] Nudata Security, Case Study: Hybrid account takeover attack at login, 2022: https://1zmiiq24oo5a7l1r624eayhp-wpengine.netdna-ssl.com/wp-content/uploads/2022/08/nds_case_study_hybrid_ato_attack_dec2021.pdf

How to address these fraud patterns?

- **We want to make the most of EMVCo's 3DS 2 support for a frictionless flow**
  - 3DS Method URL
  - Optional step where client browser opens a hidden iframe, allowing "collection code" to execute
  - If the data provided is sufficient, low risk transactions could be processed frictionless, without a challenge
  - Still a cross-origin iframe (potentially unsafe)
- **Enable detection of a known browser in a privacy friendly way: Proving a specific customer is returning on the same browser**
  - Using a challenge / response mechanism



How to address these fraud patterns?

- **Keypair bound to device hardware (WebCrypto API)**
  - WebCrypto API, supported by most browsers, allows the generation of public-private keypair
  - Relies on Crypto objects stored in browser's IndexedDB database
  - Can be marked as "extractable = false" during creation time, prohibiting the JavaScript from exporting the key. Can only use it to encrypt / sign
  - Lost when user deletes / clears browser data
  - Would be valuable if the Crypto object could be tied to hardware (Secure Enclave, TPM)
  - Could tie into the browser attestation proposal
  - Take the customer through a trust ceremony where they can opt-in to be remembered on this browser -> proceed to generate a keypair which can be used for full challenge / frictionless flow for a set period of time

How to address these fraud patterns?

- **“Trust Token” proposal from the Anti Fraud CG (Web Incubator CG)**
  - While Trust Tokens allow you to identify a good browser, we need a way to determine who it is associated with
  - If not, an attacker can open an account with bank.com, sign in on his machine, which bank.com will trust. Next time he signs in to bank.com using stolen credentials, the browser will return a valid TrustToken for the bank.com domain
  - Perhaps have a “Remember Me” process built into the browser, requiring user consent and friction the first time, having the specific user explicitly opt-in
  - The Trust Token API will therefore allow you to either issue tokens anonymously, or by passing in an ID / reference at creation time
- **Trust Tokens are valuable in the cross-origin context as well:**
  - Token issued in 1P context (bank.com)
  - Embedded iframe can redeem token during 3DS flow (acs.bank.com embedded on merchant.com)

How to address these fraud patterns?

- **“Device Integrity Attestation through the Browser” proposal from the Anti Fraud CG**
  - Already using this concept when an OOB challenge is made to customer’s mobile app (Google SafetyNet Attestation / Play Integrity API’s and Apple’s App Attest Service)
  - Allow us to assert that the customer is running an untampered version of a browser
  - If some form of hardware-attested uniqueness is present, reliance on browser fingerprinting could be reduced
  - A fine balance to not disallow browsers that are customized / have legitimate extensions installed
  - We need to explore how browser attestation could be used by the issuer during 3DS payment flows

How to address these fraud patterns?

- **“Add eTLD+1 request header to expose domain spoofing” proposal from the Anti Fraud CG**
  - Could prove useful for issuers to validate the eTLD+1 header value
  - If fraudster embeds ACS iframe on their fake storefront, the request header could be used to detect a possible fraud event, due to invalid domain embedding the ACS iframe compared to where the transaction originated from
  - Need to explore this further

How to address these fraud patterns?

- Involving the customer during a browser trust process is key. Need to be informed: similar to geo-location, password storage or SPC requests (actual modal popup)
- We require some form of identifier or credential to differentiate between a returning browser and a new browser, for a specific customer. Simply having a trusted **browser** is a step in the right direction, but a fraudster could still mark their browser as trusted on a given domain
- Browser access to hardware backed secure storage for key material & device attestation could have a big impact on the legitimacy and trustworthiness of payment credentials

entersekt

Thank you

www.entersekt.com