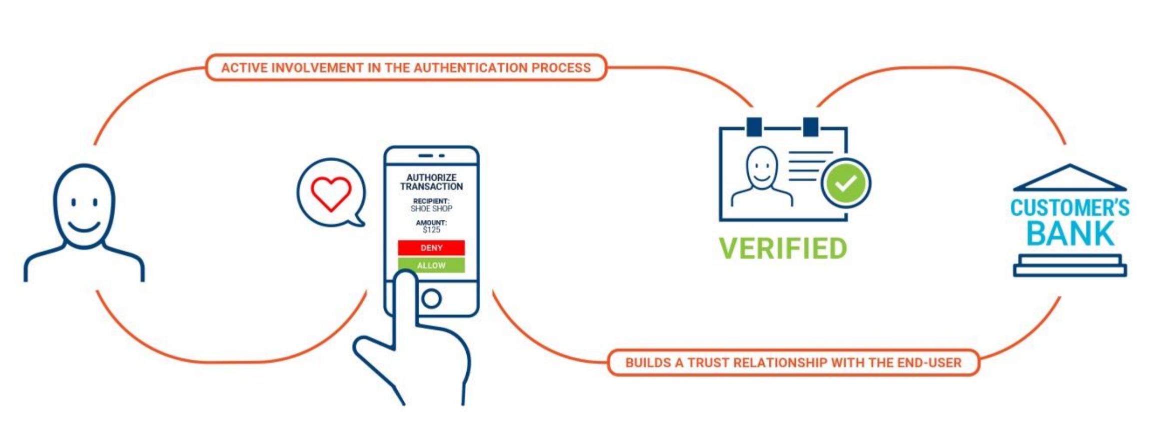
White Paper

Secure Authentication Through Active Customer Engagement


ACTIVE INVOLVEMENT IN THE AUTHENTICATION PROCESS
AUTHORIZE TRANSACTION
RECIPIENT: SHOE SHOP
AMOUNT: $125
DENY
ALLOW
VERIFIED
CUSTOMER'S BANK
BUILDS A TRUST RELATIONSHIP WITH THE END-USER

GOODE INTELLIGENCE
YOUR PARTNER FOR BUSINESS RESEARCH & ANALYSIS

Entersekt

First Edition February 2018

Published by:
Goode Intelligence

Sponsored by:
Entersekt

www.goodeintelligence.com
info@goodeintelligence.com

Whilst information, advice or comment is believed to be correct at time of publication, the publisher cannot accept any responsibility for its completeness or accuracy. Accordingly, the publisher, author, or distributor shall not be liable to any person or entity with respect to any loss or damage caused or alleged to be caused directly or indirectly by what is contained in or left out of this publication.

CONTENTS

Customers are increasingly demanding that financial institutions actively protect their digital identities and finances from rising levels of fraud. They want the visible assurance that banks and payment providers are taking the necessary steps to secure their transactions. Involving the customer in the authentication process may be just the ticket.

In an era of large-scale identity theft and increasing levels of e-commerce fraud, assuring your tech-savvy customers that their financial institution is proactively protecting their online transactions is of paramount importance. This white paper from cyber security research and consulting company Goode Intelligence details how authentication can play a role in securely identifying banks' customers.

SHOPPING WITH ABANDON(MENT)

E-commerce is exploding; yet many shoppers give up on a purchase at the last minute – a phenomenon called *cart abandonment*. In fact, the global average cart abandonment rate for 2016 was 77.24 percent – meaning over three quarters of shoppers chose to leave an online store without completing their purchase. The figures for mobile are even higher (85.65 percent in 2016).[1] Why is this?

¾

of shoppers abandon their carts before completing the purchase

Friction in the process of paying for digital goods is cited as the primary reason for cart abandonment. This friction refers to complicated checkout processes and rigid requirements such as forcing shoppers to create an account before they are able to buy something. Consumers' lack of trust, or the perception of a payment experience as "unsafe", has also proved to be significant.

[1] https://www.barilliance.com/cart-abandonment-rate-statistics/

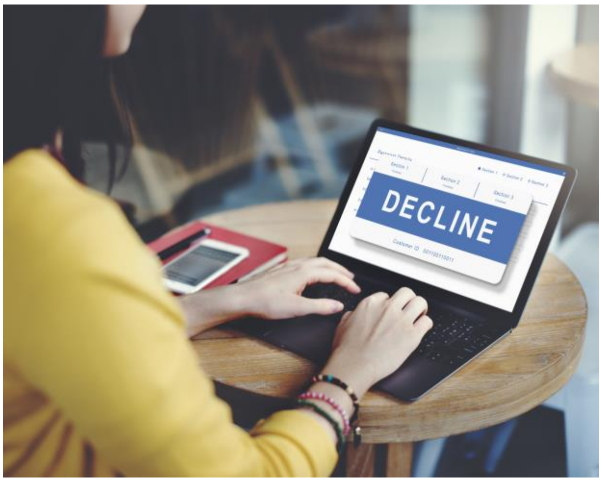
In the rush to reduce friction in their checkout processes, merchants often pursue “passive” (background) mechanisms like risk-based authentication. Risk-based fraud management makes payment authorisation decisions based on a number of signals. These risk signals can be

- device-based, e.g. the MAC address of a desktop computer, or mobile-based identifiers like an IMEI or IMSI
- network-based, e.g. an IP address
- based on geolocation or known mobile network identifiers
- based on user behaviour, e.g. when a shopper is known to often make a purchase at a certain time of day or get their goods delivered to a known address.

However, risk-based authentication can produce false declines, resulting in legitimate customers being penalised. In the so-called corridor of uncertainty, where transactions are neither obviously fraudulent nor obviously legitimate, there is a significant probability that either a fraudulent transaction will be approved or a legitimate transaction refused. Both of these can have a severe impact on the trust relationship between a financial institution and their customer, with that institution’s card being moved to the back of the customer’s wallet.

Risk-based authentication is an example of “passive” authentication, where little or no user input is required during the authentication process. Passive authentication solutions can do a pretty good job of restricting fraud, but their accompanying high false decline rates cost billions – and send users straight into competitors’ arms. BI Intelligence estimates that false declines cost the digital commerce industry $8.6 billion in 2016, and were often the result of identity-related issues. [2] Similarly, figures from MasterCard show that 39% of cardholders abandon a card after a false decline, while a quarter decrease usage. This equates to tens of billions of dollars’ worth of lost sales to merchants. In addition, 32% of online shoppers say they’ll avoid merchants that have declined their legitimate transactions before.

False Declines, or ‘false positives’, are valid transactions that are incorrectly rejected – often an unintended consequence of a merchant’s fraud prevention strategy



[2] The False Declines Report. The $8.6 billion problem that’s undermining E-Commerce Merchant’s fraud prevention strategies. BI Intelligence July 2016.

Secure authentication through active customer engagement

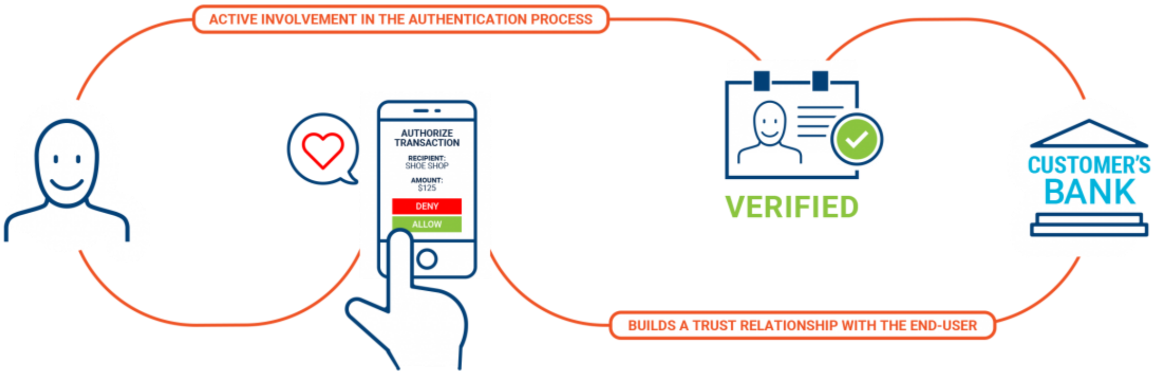
It’s a delicate balancing act: card issuers and their retail clients need to balance fraud management and customer retention whilst simultaneously increasing customer acquisition. The aim is to limit fraud in the digital channels by adopting an efficient authentication mechanism that does not unduly interfere with the user experience (i.e. by requesting additional user verification data through inconvenient methods). At the same time, recent data indicates that consumers tend to want to know that they are being protected, and want to be involved in the authentication process. American Express found in a survey that, in 2016, 37% of US online shoppers abandoned a shopping cart because they felt that the online store’s security was inadequate. Authenticating in the background, therefore, runs the risk of causing users to feel as though the security measures in place are non-existent or insufficient, rather than convenient.

The crucial lesson to be learnt from these figures is that to limit fraud *and* enable e-commerce, financial institutions need a reliable method of identifying their customers, but one which also ensures that these customers feel protected. The only way to achieve this is to establish trust between the customer and the financial institution.

39% of cardholders abandon a card after a false decline, while a quarter decreases usage.

32% of online shoppers say they’ll avoid merchants that have declined their legitimate transactions before.

GETTING THE CUSTOMER INVOLVED


ACTIVE INVOLVEMENT IN THE AUTHENTICATION PROCESS
AUTHORIZE TRANSACTION
RECIPIENT: SHOE SHOP
AMOUNT: $125
DENY
ALLOW
VERIFIED
CUSTOMER'S BANK
BUILDS A TRUST RELATIONSHIP WITH THE END-USER

Participation and Choice

In response to the current high levels of cart abandonment and false declines, there is an increasing demand for customer participation in the authentication process. Instead of being passively identified during a payment transaction, consumers want to be *actively* involved in this process, and given assurance that their digital identities – and their money – are protected. Research carried out by RSA in 2017[3] discovered that 93 percent of consumers *want* to be involved in choosing how their personal information and accounts are protected online. The same study found that 91 percent of consumers prefer a service provider who makes security visible during online transactions. Denying your customers agency in this arena is becoming less and less tolerated.

The Impact of Regulation

International regulations are also starting to encourage the active involvement of consumers in authentication - notably the European Banking Authority's (EBA) Strong Customer Authentication (SCA) Regulatory Technical Standards (RTS) in the second iteration of the Payment Services Directive (PSD2).[4]

The RTS, scheduled to come into force in September 2019, is very clear on the use of SCA for online payments within the EU, and makes SCA mandatory for accessing a payment account and authorising payments online. This means that, to prove their identity, customers will have to provide at least two out of the following three elements:

1. Something they know (a password or PIN code)
2. Something they own (a card, hard token or mobile phone)
3. Something they are (a biometric factor)

[3] https://www.rsa.com/content/dam/pdfs/5-2017/RSA-consumercybersecurity-infographic.pdf
[4] http://europa.eu/rapid/press-release_MEMO-17-4961_en.htm

ENTERSEKT'S TRANSAKT - A SIMPLE WAY TO AUTHENTICATE CUSTOMERS AND PREVENT FRAUD

Supporting customers' demand to be involved in authentication whilst at the same time finding the sweet spot between convenience and security is no small feat for a financial institution. As it turns out, there is a simple solution. One online and mobile security vendor that has managed to help banks thrive in today's increasingly challenging digital landscape is Entersekt.

PAY
$100
ALLOW
DENY
BANK

Entersekt's flagship authentication product, Transakt, solves the issue of authentication by creating a trusted channel between an organisation and its customers. This separate, end-to-end-encrypted, out-of-band channel is linked directly to their customers' mobile devices. It is also completely under the organisation's control, preventing fraudsters from eavesdropping on or intercepting communications.

Transakt's patented push-based authentication and mobile app security product leverages industry-standard X.509 digital certificates that uniquely identify each registered mobile device, transforming these devices into trusted factors of possession.

The solution works by sending push notifications to the customer, which they approve with a simple 'yes' or 'no' response. Allowing the bank customer to actively authorise a transaction – while at the same time avoiding a complicated verification process – is an important component of the user experience.

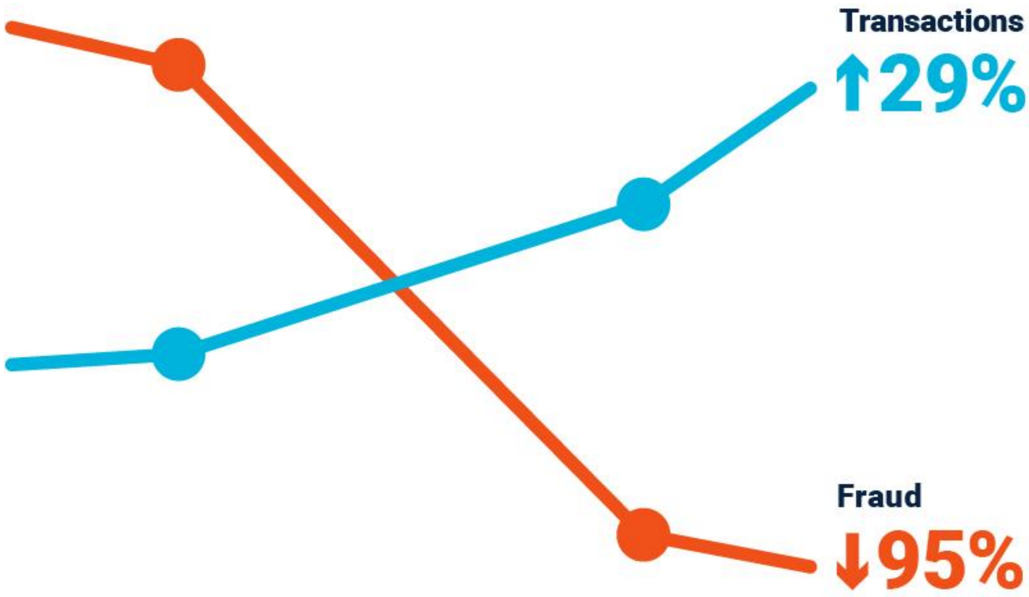
Transakt allows bank customers to:

1. View account balances and transactions
2. Create, change, or pay beneficiaries
3. Transfer funds
4. Use their credit card to pay safely and easily online

5. Digitally sign sensitive transactions
6. Send messages securely
7. Add recurring and future-dated payments

Entersekt's Transakt multi-factor out-of-band authentication product meets and even exceeds the EBA's SCA technical standards. Transakt is also FIDO U2F Certified. Today, Entersekt's patented security platform is used by millions of users in 45 countries and secures over 30 million transactions every month.

Transakt has had a demonstrable impact on fraud levels and cart abandonment at various international banks. At a German card issuer, its implementation decreased fraud by 95 percent, while successful transactions increased by 29 percent in less than 5 months. Over the same period, the issuer's revenue also increased by 15%. The one thing that *didn't* increase was card abandonment. This goes to show that a well-executed authentication solution – one that involves the customer in an intelligent way – not only reduces fraud, but also increases transaction volume.



SUMMARY

Amid the high levels of cart abandonment and false declines that frustrate merchants and customers alike, there is increasing customer demand for participation in the authentication process. With their Transakt product, Entersekt has developed an authentication solution that is as easy for organisations to deploy as it is for customers to use.

For more information on Transakt, visit:
https://www.entersekt.com/products/transakt

ABOUT GOODE INTELLIGENCE

Since being founded by Alan Goode in 2007, Goode Intelligence has built up a strong reputation for providing quality research and consulting services for the cyber security industry.

For more information on this or any other research please visit www.goodeintelligence.com.