SECUREDTOUCH

ELIMINATING ONLINE RETAIL FRAUD WITH BEHAVIORAL BIOMETRICS

Consumers are increasingly using the digital channel and the retail industry has to keep up with customers' demand for convenience. Cybercriminals are adapting their attack methods, leading to chargebacks and false positives, which translate to costly manual reviews, and blocking of legitimate users and transactions.

Credit Card Fraud

Fraudsters perform malicious activities using stolen credit card information, to make purchases and request chargebacks.

- **New Account Fraud –** fraudsters create new accounts with stolen credit cards (manually or using bots) and evade traditional fraud detection tools
- **Account Takeover –** fraudsters take over an existing account, using the real owner's credentials and abuse the credit card details, stored in the account
- **Checkout Fraud –** fraudsters use the guest checkout, to purchase with stolen credit cards
- **Bots & Emulators –** fraudsters use bots and emulators to accomplish new account fraud, account takeover and checkout fraud, through automated web injection to scale operations and increase profit

Coupon Fraud / Loyalty Fraud

Fraudsters look to gain access to coupon codes and loyalty programs points that they can use or sell to others. They use bots to scale operations, increase profit and avoid detection.

- **New Account Fraud –** fraudsters create new accounts (manually or using bots), with synthetic identities, in order to abuse coupons and free trials
- **Account Takeover –** fraudsters take over an existing account, using the real owner's credentials and abuse the credit card details, stored in the account or access loyalty points

Inventory Hoarding

Fraudsters use bots to place items in online carts, without eventually making the purchase, keeping inventory from legitimate customers.

- **Bots & Emulators –** fraudsters use bots to place merchandize in online carts, disrupting the availability of inventory

Solution Highlights

- **Lower fraud rate** by fighting multiple fraud use cases with a single solution
- Detect synthetic identities **before checkout** to avoid **chargeback**
- **Reduce false positives** by accurately detecting real users and fraud attempts
- **Lower cart abandonment** by avoiding coupon abuse

Mobile and Fraud Growth – The Retail Industry

39% of fraud losses
are attributed to identity theft, including from synthetic identities

Success rate for fraudulent transactions **30%** 2017-2018

Cost of $1 fraud to merchants 2017 **$2.77** 2018 **$2.94**

https://risk.lexisnexis.com/insights-resources/research/2018-true-cost-of-fraud-study-for-the-retail-sector

Checkout Abuse

Fraudsters make unrealistic purchases to disrupt legitimate customers' ability to buy what they wanted.

- **Bots & Emulators –** fraudsters make large scale purchases, leaving legitimate buyers with no merchandize, forcing them to buy on other digital platforms, often at inflated prices

Detecting Fraud with Behavioral Biometrics

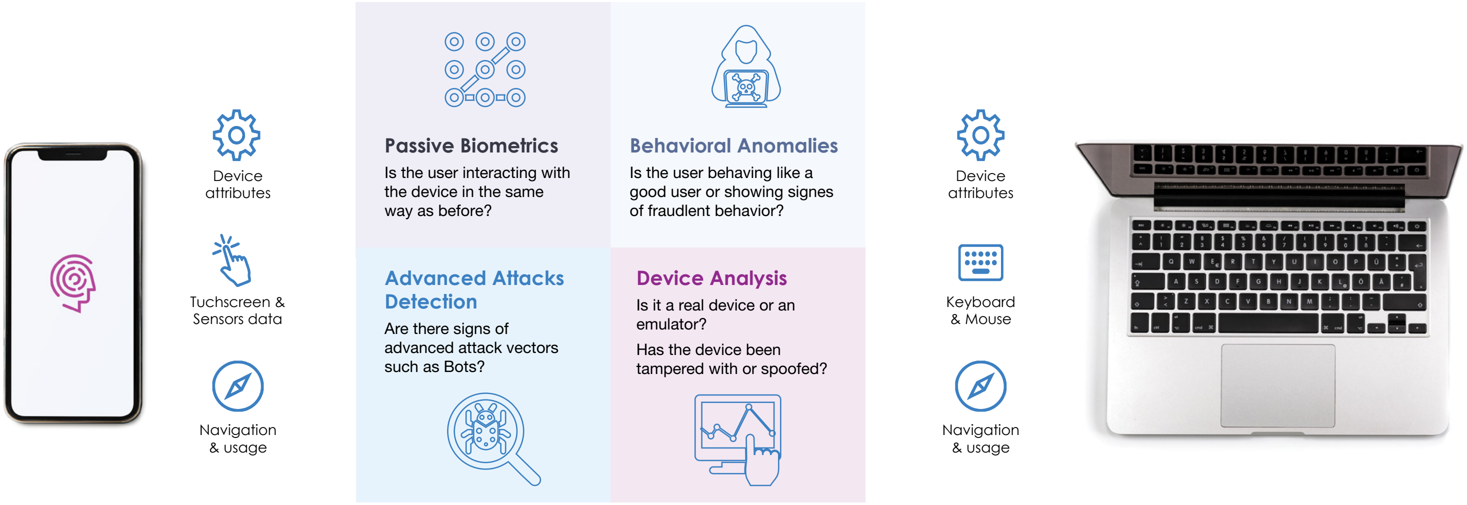
SecuredTouch accurately determines the risk of fraud in real time, lowering fraud rate by identifying fraudulent actions performed by illegitimate users, bots or emulators.

User Validation

To address the growth in fraud, online retailers implement bot detection solutions, which generate a high rate of false positives and create friction, resulting in user abandonment.

SecuredTouch applies continuous authentication, identifying trusted users throughout the entire session, eliminating step-up authentication, unless something indicates malicious activity.

SecuredTouch analyzes hundreds of machine learning features from the physical interactions between a human and a device, the device attributes and the account activities. SecuredTouch automatically identifies trusted users and flags suspicious activities, before the fraudulent activity takes place and without affecting user experience.



Device attributes

Tuchscreen & Sensors data

Navigation & usage

Passive Biometrics
Is the user interacting with the device in the same way as before?

Behavioral Anomalies
Is the user behaving like a good user or showing signes of fraudlent behavior?

Advanced Attacks Detection
Are there signs of advanced attack vectors such as Bots?

Device Analysis
Is it a real device or an emulator?
Has the device been tampered with or spoofed?

Device attributes

Keyboard & Mouse

Navigation & usage

As fraudsters adapt to the digital channels, online retailers need to ensure their customers can securely and easily make purchases.

SecuredTouch enables a unified approach to risk, addressing multiple fraud use cases in a single solution, that is frictionless to the users.

About SecuredTouch

SecuredTouch combines behavioral biometrics and continuous authentication, to detect sophisticated fraud attacks that bypass other detection tools, while ensuring a hassle-free user experience for trusted users.

SecuredTouch removes the need to choose between lowering fraud rate and a user-friendly application by conducting individual customer analysis of human, device and account activities to clearly identify the good users first.

An easily deployed light SDK solution, SecuredTouch supports both mobile and desktop environments. SecuredTouch award-winning solutions are used by clients around the world, including major financial institutions and e-commerce.

SECUREDTOUCH

Email: contact@securedtouch.com

securedtouch.com