SECUREDTOUCH

ELIMINATING DIGITAL GOODS FRAUD WITH BEHAVIORAL BIOMETRICS

The digital revolution has created a new market for digital goods, including gift cards, electronic tickets, digital subscriptions, ebooks, gaming related goods and more. Fraudsters have quickly realized the potential of this method of commerce, as the delivery of goods is immediate and the transaction is speedy and completely online.

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, avoiding the need for login credentials
- **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

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 digital goods 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
- **Avoid customer abandonment** by accurately detecting real users and fraud attempts
- **Ensure early detection** before transaction takes place

Mobile and Fraud Growth – Digital Goods

Digital goods m-Commerce adoption 57% (2017) → 70% (2018)

$1 of fraud costs digital goods merchants an average of $3.29 24% (2018)

2.1% of digital goods m-commerce annual revenues is lost to fraud

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 more goods available for purchase, forcing them to buy on other digital platforms, often at inflated prices

Detecting Fraud with Behavioral Biometrics

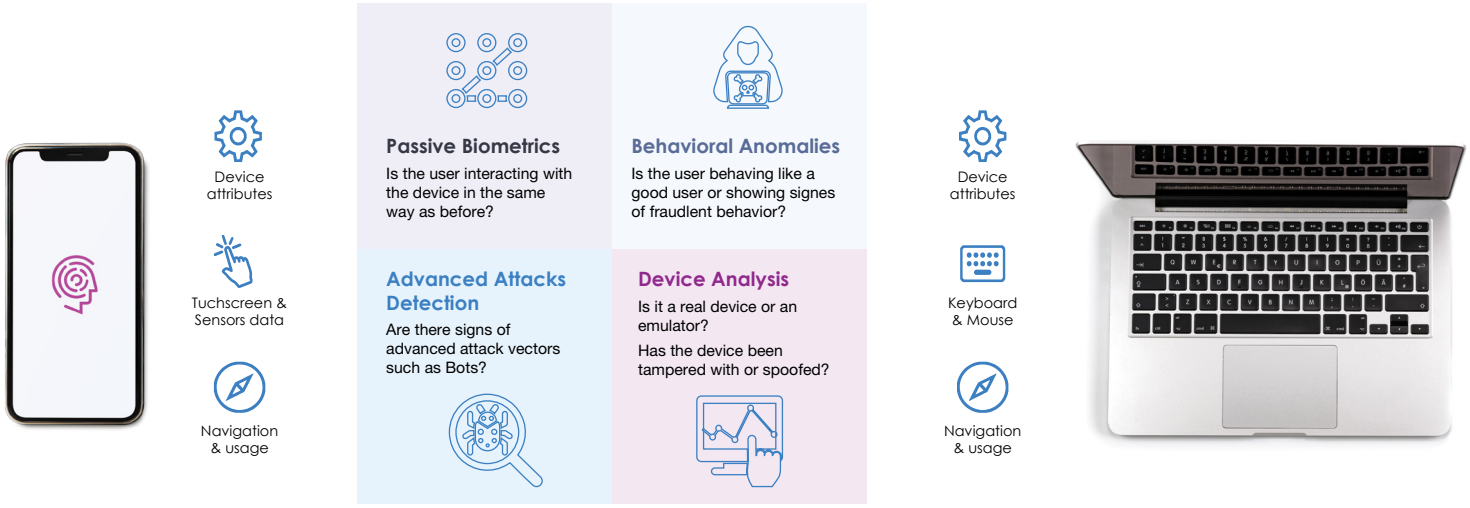
SecuredTouch accurately determines the risk of fraud in real time, lowering fraud rate by identifying fraudulent actions performed by illegitimate users, bots or emulators.

User Validation

To address the growth in fraud, digital goods providers 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.



As fraudsters adapt to the digital channels, digital goods providers 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