SECUREDTOUCH

FIGHTING FRAUD IN THE TRAVEL INDUSTRY USING BEHAVIORAL BIOMETRICS

The travel industry is unique in its attractiveness to malicious actors, with multiple fraud use cases that widen the window of opportunity for gain. The main contributors for easier gain, are the relatively high value of a purchase and the short time between purchase, and deal execution (last minute bookings).

Credit Card Fraud

Fraudsters perform malicious activities using stolen credit card information and users' credentials. They also make fraudulent chargeback requests.

- **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 account takeover through automated web injection to scale operations and increase profit

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

Coupon Fraud

Fraudsters look to gain access to coupon codes 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 to gain coupons/discount codes
- **Account Takeover** – fraudsters take over existing accounts, to access coupons received by the account owner
- **Bots & Emulators** – fraudsters use bots and emulators to accomplish account takeover through automated web injection to scale operations and increase profit

SecuredTouch identifies when a transaction is executed or a new account is created, by an illegitimate user or a bot, and not by the real account holder.

Solution Highlights

- **Lower fraud rate** – fight multiple fraud cases with a single solution
- **Avoid chargebacks** – detect automated fraud before checkout
- **Reduce false positives** – detect trusted and fraudulent users
- **Lower customer abandonment** – avoid loyalty account abuse

Mobile and Fraud Growth – The Travel Industry

Cost of fraud in the travel industry

2017 **$21B** → 2020 **$25B**

Source: https://www.enett.com/insights/fraud-form

US mobile travel sales **$75.85B** 16.7% from 2016

https://www.traveltripper.com/blog/important-mobile-booking-stats-for-hotels-in-2018/

Digital travel sales **40%** via mobile

https://www.emarketer.com/Article/Mobile-Drives-Growth-of-Online-Travel-Bookings/1016053

Mobile bookings by US travelers **72%** within a 48-hours to the booking

https://www.sojern.com/travel-insights/2018-i1

Loyalty Fraud

Fraudsters steal loyalty points to make travel and other purchases or to sell them to online brokers and other malicious actors on the darknet.

- **Account Takeover –** fraudsters take over accounts, to access loyalty points
- **Bots & Emulators –** fraudsters use bots and emulators to accomplish account takeover through automated web injection to scale operations and increase profit

SecuredTouch identifies when an account is accessed by an illegitimate user, or a bot, by recognizing when actions are not performed by the real user, or the real user's device, or when the action is performed by a non-human.

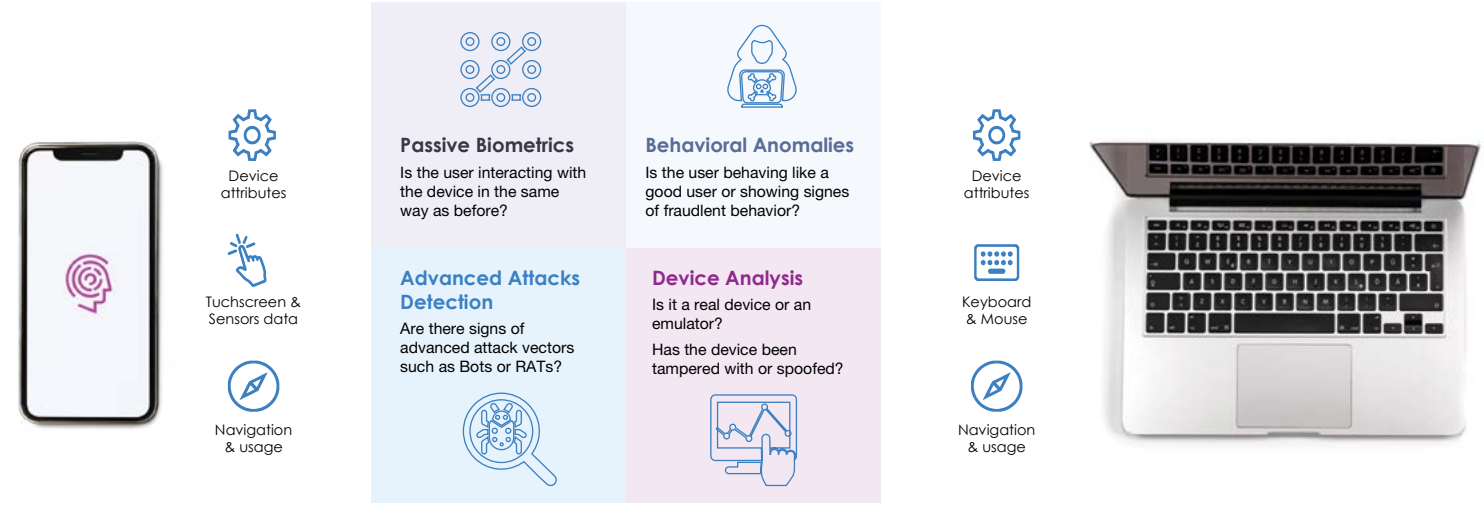
User Validation

To address the growth in fraud, online/ mobile travel businesses 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.

Detecting Fraud with Behavioral Biometrics

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, online travel businesses 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