SECUREDTOUCH

STOP NEW ACCOUNT FRAUD

WITH BEHAVIORAL BIOMETRICS

ILLEGITIMATE ACCOUNTS OPERATE UNDETECTED

Creating a new customer account should be a simple process designed to increase the conversion rate of new user registration. However, not all new accounts are created with legitimate data. Using stolen PII, fraudsters have been creating synthetic identities - or fake ones - for monetization and malice. Optimized UX for new account registration may be a necessary business need but it opens up vulnerabilities for fraudster exploitation.

STATIC INDICATORS FAIL TO DETECT FRAUD

Fraudsters use new accounts to verify and/or use stolen payment details. They have also taken this a step further by adapting their tactics to exploit loyalty program incentives such as coupons, points, and referral bonuses for signing up new users. Without a holistic view of the customer journey these behaviors lack context and the alerts to fraud occur after the incident has happened.

HIGHLIGHTS

NEW ACCOUNT FRAUD BY THE NUMBERS

✓ **$3.4 Billion** in Losses in 2018

✓ Increased over **25%** in 2019

✓ **26 Hours** Avg Customer Resolution Time

IMAGINE KNOWING FRAUD IS HAPPENING IN REAL TIME

RETAIL

DIGITAL GOODS

TRAVEL

FINTECH

DIGITAL BANKING

BEHAVIORAL BIOMETRICS IDENTIFY MALICIOUS INTENT IMMEDIATELY

This is the only way to effectively prevent malicious transactions from being completed. Long before checkout, fraudsters are giving away their intent. There are hundreds of give-aways of bad behaviors - regardless of automated (bots & emulators) or manual methods - but evident only if you know what to look for and using the right technology.

EFFECTIVELY DETECT FRAUD

Traditional tools are operating under the ancient paradigm of a single gate keeper. Our current digital age requires a tool that has the ability to see, gather, and analyze user behaviors across the entire customer journey.

USER JOURNEY

Fraudsters are mission-oriented and repeat a tried and tested deception path

HUMAN BEHAVIOR

Real users exhibit identifying traits such as unique vibrations, velocities, angles, and timing limitations

DATA FAMILIARITY

Fraudsters copy & paste address fields instead of using autofill or smoothly typing a username or password

FRAUDSTERS SEND DATA SIGNALS THE MOMENT THEY ENGAGE

Fraudsters leave behind a trail of behavioral breadcrumbs. These breadcrumbs may be tiny but represent a set of granular data points that until now have been ignored. SecuredTouch's power comes from leveraging these defined and measurable sets of behavioral patterns with proprietary machine learning algorithms. A complete view of the user's behavioral journey allows a frictionless, accurate, and scientific approach to fraud detection. SecuredTouch provides unique pre-trained behavioral models and dedicated models that are trained per customer. This flexibility allows detection of bot, emulator, and manual attack behaviors. Regardless of control weaknesses that may have been overlooked on a website or app, SecuredTouch is learning, watching, and providing real time detection before any transaction is completed.

CAPTURE THE ENTIRE FRAUD FLOW

Fraudsters target digital properties armed with stolen PII including payment details, a plethora of tired-and-tested automated and manual attack methods to easily create new accounts.The path to monetization and malice is quite easy. SecuredTouch understands user intent behind every step of the new account fraud flow and empowers fraud analysts to prevent incidents from completing.

SOLUTION HIGHLIGHTS

POWER OF MACHINE LEARNING

- ✓ Analyzes Thousands of Data Points
- ✓ Pre-Trained Models
- ✓ Custom Models Trained for Clients
- ✓ Stays Ahead of Fraud Trends
- ✓ Responds in Real-time
- ✓ Early Detection
- ✓ Reduce Manual Reviews

COMPLETE COVERAGE OF YOUR USER'S JOURNEY

- ✓ Seamlessly Monitors Usage Patterns Throughout the Journey
- ✓ Provides a Risk Score Before any Transaction was Made (and Before Registration is Completed)
- ✓ Provides a Risk Score Even When There's no Transaction

THE ULTIMATE GUIDE TO
ECOMMERCE FRAUD
DOWNLOAD THE WHITEPAPER

FURTHER READING

The Ultimate Guide to Fighting eCommerce Fraud in 2020

Improving fraud detection in a consumer driven market is no easy feat.