SECUREDTOUCH

PREVENT ACCOUNT TAKEOVER

WITH BEHAVIORAL BIOMETRICS

Traditional solutions do not have visibility into early touchpoints in the digital customer journey. Don't be the last to know an account has been compromised.

CUSTOMER VS. FRAUDSTER

Without complete visibility into user behavior, fraudsters can penetrate user accounts pretending to be a legitimate customer and successfully purchase goods and services without being detected. Traditional solutions focus on static, and historical data points that cannot provide visibility into behavioral patterns across the entire customer journey, resulting in fraud being identified after the fact. Machine learning tools provide the capability to identify fraudsters before they complete their attack.

EXPLOITING THE BLINDS SPOTS OF THE USER JOURNEY FOR ILLEGAL PROFIT

The increasing sophistication of credential stuffing tools in combination with the volume of stolen PII available makes attacks inevitable. Once an account has been taken over, fraudsters will use different monetization techniques, such as purchasing through stored payment, changing the shipping address, or scraping and reselling user PII on the dark web. Blocking this fraud without sacrificing user experience is challenging. In some instances, this behavior is impossible to detect when you are relying on a transaction analysis based solution. We are seeing more instances where fraudsters complete their task without making any transactions at all.

HIGHLIGHTS

ACCOUNT TAKEOVER BY THE NUMBERS

- **2+ Billion** stolen credentials on dark web shops
- **$4B Lost** to ATO in 2018 alone
- An attack costs victims an average of **$290** and **15 hours** to resolve
- Account takeovers are up **79% in 2018**
- Bots can be purchased for as little as **50¢ on the dark web**

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 and continuously assess the risk, without waiting for a transaction to happen.

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

MALICIOUS INTENT CAN BE IDENTIFIED THE MOMENT FRAUDSTERS TAKE OVER AN ACCOUNT

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. A complete view of the user's behavioral journey allows a frictionless, accurate, and scientific approach to fraud detection. SecuredTouch can be trained to use a unique behavioral model or operate on a pre-trained model suitable for the client's digital environment. The solution's power comes from the flexibility of leveraging a broad variety of behavioral data with proprietary machine learning algorithms. 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.

REDUCE FRAUD LOSSES WHILE INCREASING CONVERSION RATE AND CUSTOMER TRUST

SecuredTouch has witnessed the creativity of fraudsters' attack journey. Recently, we saw how a weakness in control features was exploited. Account settings had allowed users to set notifications for account activities yet there was no notification check for turning the notifications off. This provided an easy path to monetization. But with SecuredTouch in place, this type of behavior, along with many others, is fed into the ML models and could help detect an anomaly and stop the fraudulent user from committing malicious activity.

SOLUTION HIGHLIGHTS

POWER OF MACHINE LEARNING

- Thousands of data points
- Pre-trained ML models
- Adapts and gets smarter
- Stays ahead of fraud trends
- Real-time detection
- Reduce manual reviews

COMPLETE COVERAGE OF YOUR USER'S JOURNEY

- Engages the moment user logs in
- Continuously gathers hundreds of behavioral touchpoints
- Detection and prevention in real time, before checkout
- Delivers risk scores in real time
- Customizable risk thresholds to reduce UX friction

FURTHER READING

An eCommerce Showdown: Account Takeover VS Behavioral Biometrics

When it comes to eCommerce fraud, account takeover (ATO) is at the forefront of attacks.
https://blog.securedtouch.com/ecommerce-account-takeover-vs-behavioral-biometrics