

Gett fights emulator-based New Account Fraud

with Behavioral Biometrics

↓ 01 Initial situation

Just as consumers are increasingly using their mobile phones for all types of financial transactions, cyber criminals are turning their focus to new mobile fraud attack techniques.

Gett's fraud team became concerned about New Account Fraud (NAF) and credit card fraud. NAF occurs when fraudsters open new accounts with illegally-acquired real credit card information sourced from the Dark Net, which are then recognized as valid. Previous fraud prevention solutions can detect and block such fraud, but only if real devices are used.

However, Gett has been confronted with an increasing number of emulator-based fraud cases which fake real devices. Not optimized for this type of attack, Gett's previous fraud detection solutions had to adapt to a new threat landscape based on simultaneous use of valid, albeit illegally-acquired credit card data.

The use of stricter rules led to an increasing number of false positives, leading to the unnecessary blocking of legitimate users – resulting in dissatisfied customers and lost profits. The company was anxious to find a solution.

Behavioral Biometrics proved to be the optimal fraud detection solution best suited to mitigating this new generation of sophisticated fraud attacks.

"Once we realized that we were exposed to fraudulent activity that we were not detecting in a timely manner, we looked for a new detection technology altogether. The Behavioral Biometrics solution instantly showed us what we knew was there but had no ability to identify – emulator-based fraud. Having the visibility and technology to prevent a significant part of our fraudulent activities translates into a great ROI."

Guy Douek, Global Head of Payments, Gett



About the client

Available in more than 120 cities worldwide, including London, Moscow and New York, Gett is the global leader in the corporate on-demand transportation market.

Gett Business Solutions is the only global corporate transport solution, enabling companies and riders to book rides and track expenses worldwide through a single platform. It is already used by more than 20,000 companies worldwide who book and track transportation services in over 1,000 cities and 56 countries.



↓ 02 The solution and how it works

Our platform seamlessly detects mobile fraud attempts that apply sophisticated virtual and automated fraud techniques using fraud-focused emulators, bots, malware and Remote Access Trojans (RATs) to undertake fraudulent activities.

Our solution uses behavioral biometrics technology, designed specifically to prevent mobile fraud, by analyzing interactions between humans and their mobile devices. As each human has a unique way of holding and using their device, the emulator can mimic the device, but not the human to device interaction.

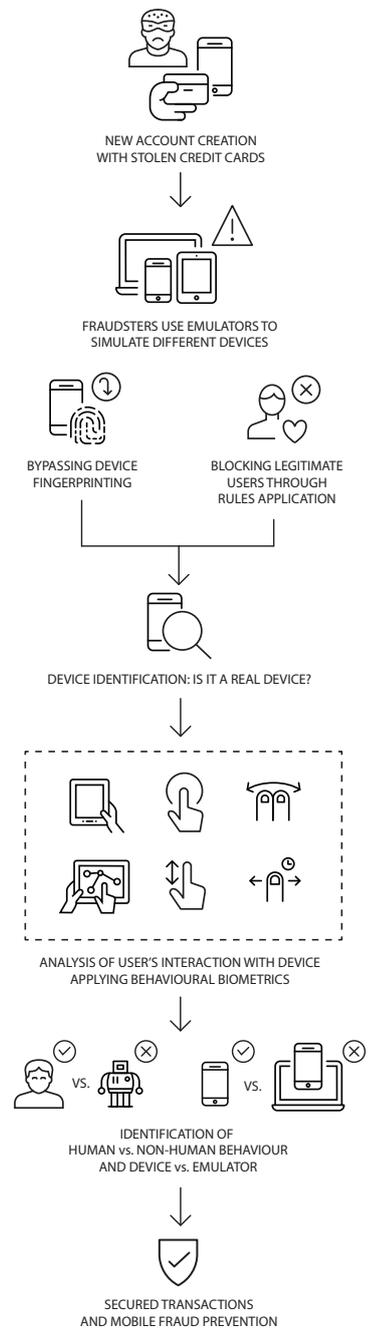
Be it the way a person grasps the mobile device, the pressure the finger applies, the finger size or the speed of swiping – these parameters and hundreds of machine learning features, are used to automatically differentiate between human and non-human behavior, and device vs. emulator, making the process of securing a mobile transaction quicker and more accurate.

Using behavioral biometrics, our platform automatically identifies and repels attempted fraudulent transactions. Learning from previous attack behaviors and attributes, we ensure early detection of emulators and bots that use legitimate data such as user credentials or valid credit card details, to prevent fraudulent new account enrollments. This mitigates fraudulent damage without impacting the true legitimate identity owner.

↓ 03 The result

- Plug-and-play solution preventing fraud, while enabling a frictionless user experience.
- Once deployed, the platform was instantly operational with no need for baseline profiling in order to start its automatic monitoring activities on-the-go and the discovery emulator usage.
- Discovery of emulator sessions that were bypassing existing fraud detection tools.

The fraudulent activities detected by our solution amounted to a decent portion of the overall fraud attacks. These attacks went undetected by other solutions and the emulator attacks were not visible in real time to the fraud team, until our platform had been installed.



Our Services

Evaluation of existing risk and fraud detection tools by industry experts, considering the client's whole digital value chain

Analysis of present threats and fraud patterns to determine and execute optimizations to the existing fraud prevention setup

Simple solution integration in the given fraud prevention architecture, through a passive deployment without active enrollment from the end user

A solution in cooperation with  SECUREDTOUCH

Arvato Financial Solutions is partner and shareholder of SecuredTouch

Would you like more information? Feel free to contact us.

Arvato Financial Solutions | Sales Team Fraud Management
Telefon: +49 7221 5040 - 1600 | fraud-management@finance.arvato.com

finance.arvato.com

