SECUREDTOUCH

CASE STUDY

GLOBAL ON-DEMAND TRANSPORTATION COMPANY FIGHTS NEW ACCOUNT FRAUD

THE CHALLENGE

An evolving range of new account, credit card, and other fraudulent activities that could not be detected by classic fraud detection tools.

THE SOLUTION

The SecuredTouch platform looks at physical device characteristics in combination with behavioral biometrics to automatically identify and repel fraudulent activities.

THE OUTCOME

The SecuredTouch platform has increased detection of suspicious activities that were invisible to classic fraud detection tools by more than 120 percent.

Gett

Gett launched one of the first-ever on-demand B2B mobility services in 2010. Their advanced technology makes business ground travel simpler, safer, and more efficient. Gett's software powers, among other clients, a third of the Fortune 500. The company believes in a future where our software helps businesses thrive, by empowering people to be their best on the go.

ONE CLIENT, 5 USE CASES SOLVED

EMULATOR BASED FRAUD

NEW ACCOUNT FRAUD

CREDIT CARD FRAUD

DEVICE BASED FRAUD

SHADOW APPS DETECTION

Gett is a corporate transportation company that connects private and corporate riders with ground travel and delivery services. The company operates in Israel, the UK, and Russia. As a software as a service (SaaS) solution, Gett consolidates collections of vendors on a single booking platform while clients access this service using apps for iOS and Android.

Initially, Gett reached out to SecuredTouch because they had a problem with emulator-based new account fraud. Once SecuredTouch addressed this issue, fraudsters pivoted their attack methods, presenting Gett with more intricate fraud flows originating from real devices, employing more advanced evasive manipulations to device attributes. Gett needed a solution that could adapt to these evolving tactics and flag suspicious activities before transactions were completed. The solution needed to be implemented quickly and be up and running as soon as possible.

SECUREDTOUCH QUICKLY IDENTIFIES INCREASINGLY SOPHISTICATED NEW ACCOUNT FRAUD SCENARIOS

THE FIRST ATTACKS USED EMULATORS

Gett's fraud team initially experienced new account fraud (NAF) and credit card fraud executed using emulators. These emulators allowed fraudsters to mimic devices to commit fraud easily and scale their activities efficiently without large investments in devices. Rides were paid for using stolen credit cards acquired from the Dark Web. Gett contacted SecuredTouch to gain visibility into the scale and extent of these emulator attacks as well as identify fraudulent sessions so they could stop them.

SecuedTouch's device intelligence solution identified these emulators using Behavioral Biometrics. The analysis looked at correlations between device attributes such as battery, gyroscope, and storage that indicated the use of an emulator. Gett received real time alerts that allowed them to block these fraudulent activities before the transaction was completed.

ONCE DETECTED, ATTACKS EVOLVED

With their emulator-based attacks successfully blocked, fraudsters leveled up their assaults. They chose three further methods that took advantage of real devices instead of emulators -- sophisticated manual tactics using real devices, shadow apps that used messaging services to automate fraudulent ride requests, and manipulation of device attributes.

USING SOPHISTICATED MANUAL TACTICS AND REAL DEVICES

In their second iteration of attacks, fraudsters used real devices and adopted techniques that would avoid tripping any suspicious activity alerts. They either created new accounts and let them sit (e.g. "aged" them) or they took real rides in order to build account reputation. Only then would they add multiple credit cards to the accounts or use them to make small purchases to validate stolen credit cards. These tactics allowed fraudsters to hide their activities from detection algorithms that weigh actions taking place when an account is first created more heavily than those that occur in more established accounts.

SecuredTouch added their behavioral anomalies solution to the previously deployed device intelligence solution to detect these fraudulent activities. These solutions looked at fraud indicators to identify any suspicious behavioral or usage patterns within the user journey throughout the Gett app. More specifically, the solution analyzed the correlation between Behavioral Biometrics and shared device identifiers.

USING SHADOW APPS AND AUTOMATED MESSAGING SERVICES

In the next iteration of attacks, fraudsters used an advanced NAF monetization scheme that manipulated user and session data to evade detection. Fraudsters created shadow apps that mimicked Gett's UI, advertised low prices and then automated the ride request to Gett using messaging services—in this case Telegram. To Gett, it looked like these ride requests were coming from many users in many locations, when in fact, these orders all originated from the same device. The fraudulent app would then take a below-market-rate payment from the customer while the fraudster paid Gett using stolen credit cards. The fraudster was paid 'legitimately' through the shadow app and Gett dealt with the fallout when the legitimate cardholder requested a chargeback from the unauthorized transaction on their app. In some cases, even the driver was in on the scam.

SecuredTouch's device intelligence solution detected this bogus app scheme by identifying gaps in data it was receiving that were due to the fact that the devices the fraudsters were using didn't have the standard attributes typically found on a standard mobile device. SecuredTouch also made correlations between users, devices, and sessions. These techniques showed large numbers of taxi orders allegedly coming from various users and locations that all used the same device. SecuredTouch flagged these anomalies, allowing Gett to stop this attack method.

MANIPULATING DEVICE ATTRIBUTES WITHIN REAL DEVICES

SecuredTouch started to receive alerts that indicated device manipulation. Upon closer inspection, it was discovered that fraudsters had begun using specialized apps to change indicators on Android devices --such as device ID, and device type-- to make it look like different users on different devices were performing transactions. Fraudsters know that use of the same device to create an account, use different accounts or add multiple credit cards, sometimes in rapid succession, are strong indicators of fraud. After all, no normal user would do this. Therefore, fraudsters used this technique to manipulate device data in an attempt to circumvent Gett's security layers.

But they were unable to manipulate the device footprints. As a result, SecuredTouch easily detected attacks by uncovering devices being used in large numbers of access attempts. SecuredTouch's Device Intelligence module then used data about device changes to improve the precision of Gett's custom algorithms so they could more readily uncover these instances.

OUTCOME: DRAMATICALLY INCREASED FRAUD DETECTION

With each new generation of fraud, SecuredTouch captured increasing numbers of suspicious events. By detecting new account fraud with emulators, fraud detection increased by 62 percent. As fraudsters became more sophisticated, SecuredTouch evaluated more behavioral features and was able to double that recall.

FURTHER READING

eBook: Breaking Down Fraud Flows

Read more about the advanced tools & strategies fraudsters are using to perpetuate fraud.