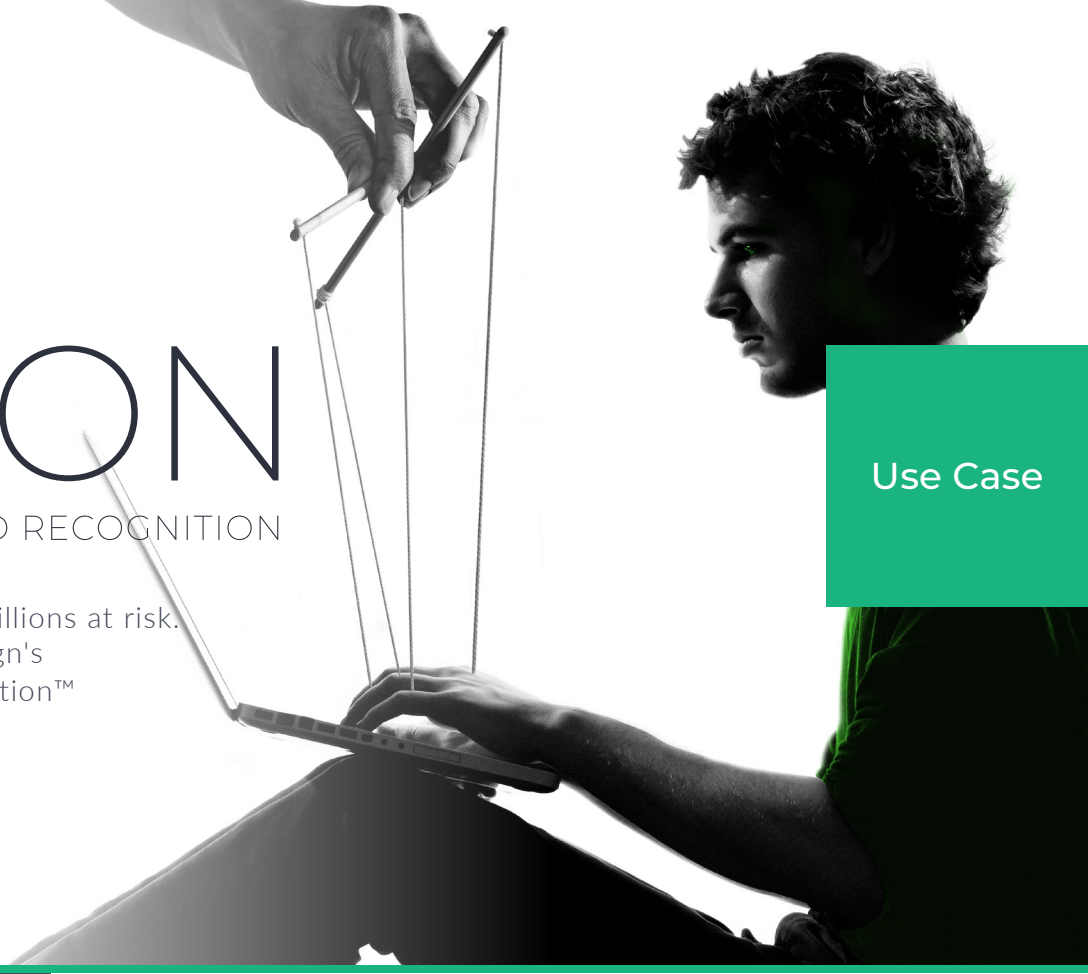
callsign®

GET ON

INTELLIGENCE BEYOND RECOGNITION

Extensive data breaches put billions at risk.
Proactively defend with Callsign's
Intelligence Driven Authentication™



Use Case

What is Account Takeover?

It is a form of financial identity theft. Whilst bank or credit card account takeover has been the subject of many headlines, other forms are growing at an even greater rate.

For example, loyalty schemes for airmiles or hotels, are now targets for the bad guys.

Social engineering is the most common way of collecting enough data to mimic a user's identity.

Victims may not detect that their account has been taken over for months. At that point they may have lost a substantial part of their account balance.

What is Account Borrowing?

Not all account takeover is committed by anonymous 3rd parties for financial gain, account borrowing is a big cost to business too. It can be explicitly borrowed, like Netflix accessed by friends and family.

It can also be using an account from an unauthorised location. For example watching a favourite program on holiday may incur licensing or copyright issues.

Account borrowing can also occur without permission, e.g. by teenagers using parental accounts.

What is First Person Fraud?

This occurs when a person or group defrauds a company using their own account. It can be making a false insurance claim, or claiming account takeover where none occurred.

Account Takeover

Account Takeover is a great business to be in – if you are one of the bad guys.

Imagine the recruitment ad:
- Run a global business from anywhere on the planet
- Flexible hours
- Gullible and trusting customers

Remuneration? Well, let's just say it is in the hundreds of millions...

What self-respecting profiteer wouldn't sign up?

And that is the challenge for any company whose business involves digital account management. Especially if you throw in customers who expect you to know they are who they say they are, but also know when it is a bad guy who just happens to know all their email, passwords and get around any biometric tests.

Who bears the burden if an account has been taken over? It is rarely the customer.

And then there is account borrowing. Well that isn't too bad really is it? You don't get any customer complaints over account borrowing, not when customers are complicit. The cost to your business is high, especially if it involves breaking copyright licensing laws.

At least where first person fraud occurs you can recoup the costs. As long as you can prove it...

> At the heart of these challenges is the need to prove someone is who they say they are, where they say they are, doing what they say they are doing. Checked and verified to keep them safe, or held to account.

Is your organisation facing an Identity Paradox?

Until now organisations believed it was impossible to satisfy the conflicting needs of security, accountability and privacy.

Regulators

Regulators are enforcing compliance with regulations like GDPR and PSD2.

Organisations

Organisations need to keep identity data safe and be accountable for doing so.

Users

Users want increasingly seamless, friction-free authentication journeys.

How can Callsign help prevent Account Takeover?

Callsign's Intelligence Machine can pinpoint potential fraudsters at the point of entry by:

Real-time Identification

Correlating the location, devices and behavior of applicants, and identifying BOTs.

Step Up Authentication

Whenever new beneficiaries are added especially with high value transactions.

Ensure Accountabillity

By being able to prove who made the transaction you can avoid the costs associated with disputed claims.

Callsign changes the rules of identity. By using all of the thousands of data points available, such as typing or swiping techniques, location, online habits, face recognition, devices, and yes, even passwords, we can determine someone is who they say they are. We even know the Monday person can behave differently to the Friday person.

Most of these data points are friction-free for the user, and so we use these to determine that someone's behaviour is within their normal pattern. Where there is a veering from the norm, we then intelligently introduce further tests, avoiding a rules-based approach that can be replicated by the bad guys. We have the lowest false positive rates in the industry, and zero breaches thanks to our inbuilt trust engine. As a result, users can get on with their digital lives whilst businesses improve customer engagement, increase productivity and reduce the risk of fraud.