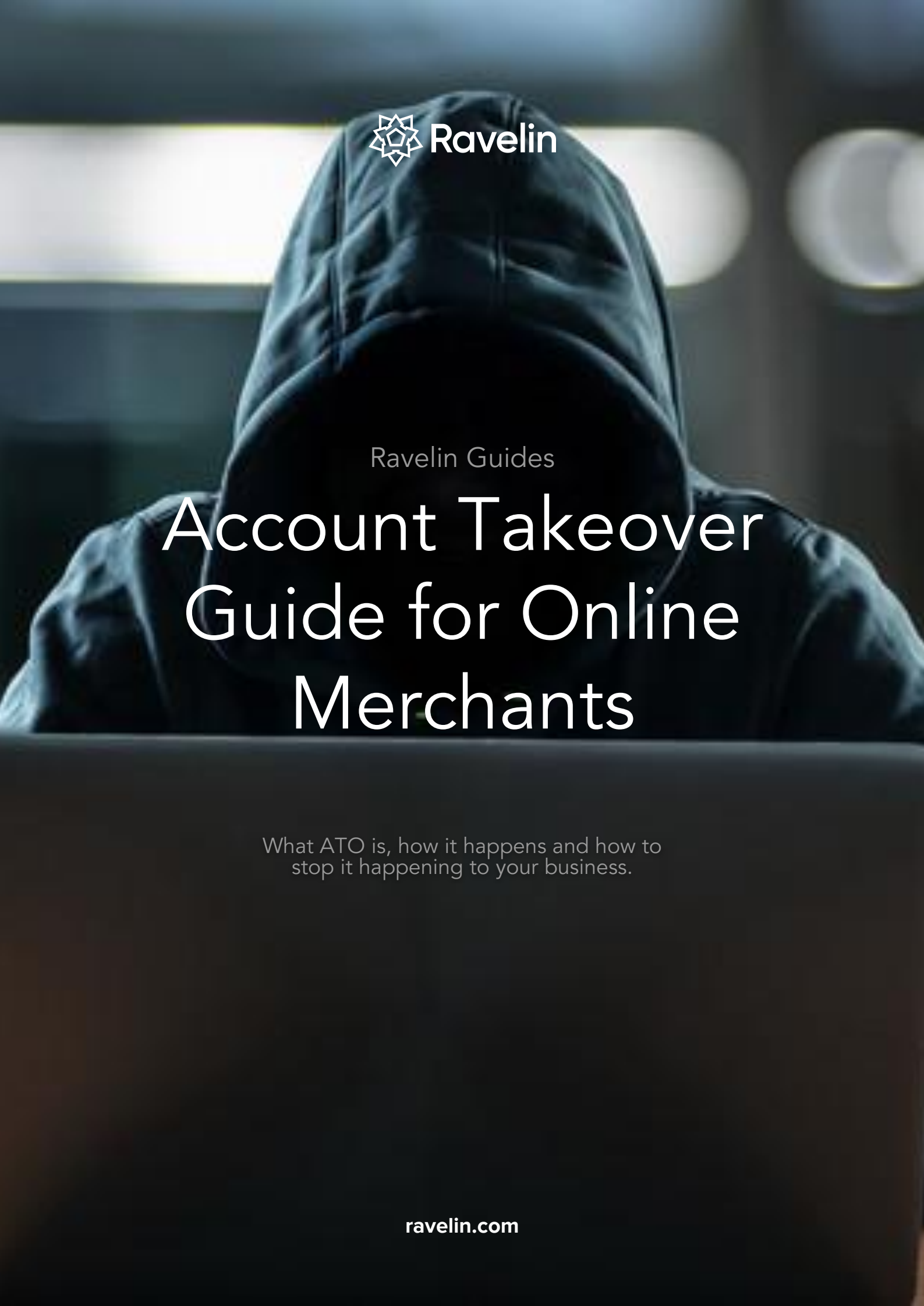


Ravelin

Ravelin Guides

Account Takeover Guide for Online Merchants

What ATO is, how it happens and how to stop it happening to your business.

ravelin.com

Introduction

The number of data breaches has been a key factor in driving account takeover. Breaches provide the means to commit the crime that is plaguing online businesses by eroding trust and the bottom line.

Fraud strategies must evolve to mitigate the risks associated with account takeover. This guide provides a summary of what account takeover is and crucially how you can protect your business from it.

Data records lost or stolen since 2013

13,443,149,623

The Data Breach Level Index

What is Account takeover?

Account takeover (ATO) is when a fraudster gains control of an account that belongs to a genuine customer. Fraudsters use the customer's good track record to make unauthorised transactions.

This can be done with the good customer's saved card details or with stolen card details purchased online. The underlying motivation for an attack can be personal use e.g. the fraudster wants access to a 'free' product or service.

Fraudsters can also change details associated with the account and sell the account on to someone else. In addition, fraudsters can monetize personal information by scraping details out of customer accounts to pass on to other bad actors.

Cybercrime can be leveraged as a service for other criminal groups e.g. fraudulently booked hotel rooms can then be sold on to other crime groups who can use it for drug trade or human trafficking.

ATO attacks can involve more sophisticated techniques such as phishing and malware however the most common method used is credential stuffing.

Credential Stuffing

Credential stuffing relies on using large volumes of stolen usernames and password combinations to automate login requests in order to gain access to users accounts. Stolen credentials can be purchased on the darkweb, shared via cracking forums (see Sentry MBA sections below) or obtained through hacking.

Credentials are also shared for free via forums. These free file dumps are likely based on older breaches that have outlived their monetary value for the sophisticated fraudsters behind the initial attack. Bad consumer habits on password security means even older dumps are still likely to see some success.

Credential stuffing relies on 'combo lists' - lists of passwords and emails usually compiled from several breaches. The combinations are then automatically run against a login with any successful attempts logged.

Credential stuffing can be scripted by more skilled fraudsters. However, automated tools make credential stuffing attacks very easy for anyone to do.

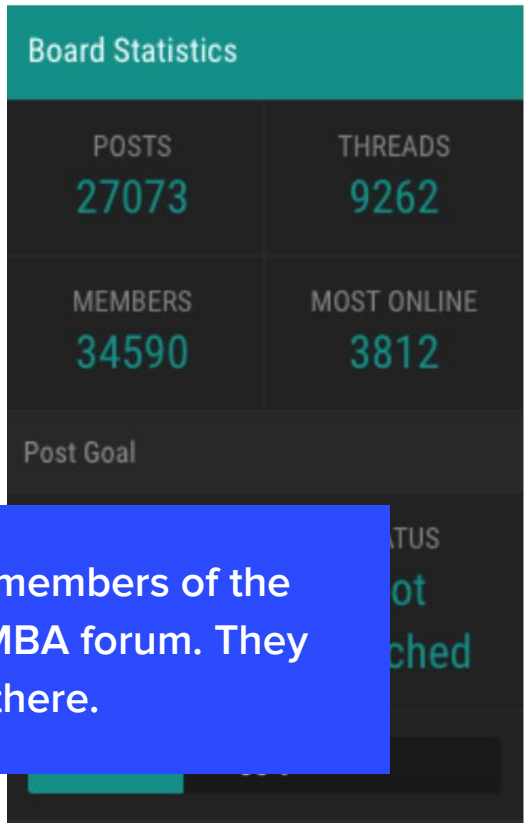
The Lifecycle of Breached Credentials

Breached credentials have a life cycle of utility for different actors. Sometimes an initial breach doesn't hit the dark web or forums for a significant amount of time. It's likely that whoever successfully caused the breach, works to get as much as they can out of the data before they sell it on for wider use. This part of the life cycle is likely dedicated to professional hackers.

On average it takes 15 months for a breach to become public knowledge. The longer it takes to discover a breach the more time fraudsters have to monetize ATO.

Once breached credentials have been sold a few times, it inevitably ends up getting posted for free in a forum (often by a script kiddie looking to build a reputation) where it can get picked up by people who are more likely to be trying to get access to a 'free' product or service.

Inevitably, the success rate of attacks likely drops off throughout the lifecycle as the company involved in the breach as well as the public become aware of the incident.



Using Automated Tools to 'Crack' Accounts

There are a range of bad actors who commit ATO from one person attacks involving easy to use automated tools like Sentry MBA through to more advanced criminal organisations.

Credential stuffing that relies on automated tools is generally known as account 'cracking'. It is incredibly easy to use an attack tool to crack an account. Fraudsters who rely on automated tools are generally not viewed as 'hackers' within the hacking community and are referred to as script kiddies because they lack the expertise to write their own script to use for hacking.

Bad actors who rely on automated tools in this way are often low level fraudsters, many of whom may just want to access a 'free' product or service through an account for personal use. Obviously, not all attacks using an automated tool originate from low-level fraudsters. Other kinds of fraudsters also rely on this method because it's easy and unfortunately, it works.

However, more advanced attackers are likely to have some kind of coherent strategy. For example, they may make their attack slot in with a seasonal trend, use botnets and craft their scripts to operate within known limitations such as IP rate limiting.

Like lower level attacks, they can use breached credentials and run scripts against targeted websites. More sophisticated fraudsters can also obtain hashed files of passwords (either themselves or on the dark web) and then decipher the passwords themselves, they don't rely solely on the more commonplace combo lists like lower level fraudsters may.

Generally, more sophisticated attackers have far more varied ways of getting credential combos to successfully commit ATO. For example, by using malware, phishing and brute force attacks.

Sentry MBA

Sentry MBA is touted as the most popular credential stuffing account tool and there is an active 'community' forum that provides support, including training.

You only need 3 things for Sentry MBA to crack accounts.

Configuration file - The config file outlines the unique characteristics of the website you are trying to hack. For example, it'll specify the URL for the login site and what fields are required.

Proxy file - This is a list of IP addresses to route traffic through to make it look like the login attempts are coming from a large variety of sources instead of a single attacker. This allows a fraudster to do a 'low and slow' attack mimicking normal traffic.

Combo list - This is a file containing the username and password combinations that are often obtained from breaches and then shared on the dark web or in cracking forums.

Fraudsters can also configure Sentry MBA to bypass captcha challenges by leveraging Optical Character Recognition (OCR) functionality. There are also a number of readily available tools like GSA Captcha Breaker and DeCapcher that can solve captchas.

Avoiding Detection

Hackers can acquire thousands of IPs that can masquerade as legitimate traffic in 'low and slow' attacks. Most businesses or their ISPs have a limit on the amount of traffic they accept from a single IP in order to avoid a malicious attack. This is rate-limiting. But you can rent a botnet for $2 an hour with access to 1,000 machines. This can impede rate limiting and/location based rules because the traffic now looks normal and like it's coming from a large number of locations or IP addresses.

Hackers also use other tricks to go undetected, like headless browsers. Headless browsers were legitimately developed to automate testing of web applications. They are often open source tools and can be repurposed to simulate real browser functionality for fraudsters. This makes their requests look like they come from real browsers not scripts but without having to actually run a full browser.

Thanks to OCR (optical character recognition), hackers can bypass captchas.
In some cases, thanks to overlays and other malware, even SMS-based 2 Factor Authentication (2FA) can be worked around by more sophisticated crackers.

The Cost of ATO

Over the last few years there have been significant increases in ATO attacks. In the US alone, Javelin Research estimates suggest that ATO cost merchants more than $5 billion in 2018.

For merchants, it's not just the cost of replacing goods or refunding payments - it's also the time spent by support and operations teams dealing with angry customers and tackling the legal and operational consequences. Your customers are also hit by ATO, spending hours to resolve the issue and often ending up out of pocket as a result of an attack.

Consumers are increasingly aware and concerned about ATO thanks to high profile data breaches. For merchants the financial and reputational costs of ATO seem to be increasing.

Javelin Research infographic on the cost of fraud

Stopping ATO

There are a number of things merchants can do to mitigate against ATO. Targeting the tools and techniques that fraudsters use to commit ATO is a good place to start.

For example, by default Sentry MBA uses the following five user agent strings:

1. Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0; .NET CLR 1.1.4322; .NET CLR 2.0.50727; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729)
2. Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; .NET CLR 1.1.4322; .NET CLR 2.0.50727; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729)
3. Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.0.11) Gecko/2009060215 Firefox/3.0.11
4. Mozilla/5.0 (Windows; U; Windows NT 5.1; en) AppleWebKit/522.11.3 (KHTML, like Gecko) Version/3.0 Safari/522.11.3
5. Opera/9.80 (Windows NT 6.0; U; en) Presto/2.2.0 Version/10.00

You can change the user agent strings within Sentry MBA, but some crackers likely don't so these strings may appear in logs and indicate an automated attack.

If you decide to target these user agent strings, it's worth considering how fraudsters may respond. Outright blocking them may just force a fraudster to change the string to something unidentifiable - it may be better to monitor which accounts are being accessed this way and prompting the legitimate owner of the account to reset their password.

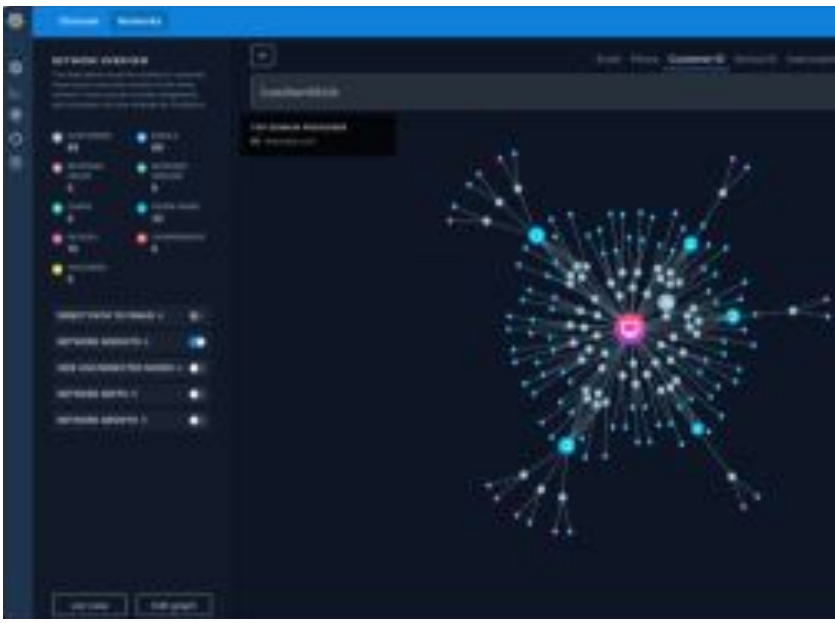
Additionally, you should monitor things like HTTP client, IP, user agent and device details and track any patterns or anomalies. Monitoring breached credentials available in the wild can also help to protect your customers from ATO. Implementing 2FA if you have verified numbers associated with accounts can be helpful though may also negatively impact conversion if applied to all customers.

Targeting other tools that may indicate suspicious activity such as headless browsers, automated OCR tools (if you use captchas), TOR, VPN, proxies etc. is also advisable.

Using Ravelin Connect to uncover ATO

Ravelin Connect is a graph network that is used to identify significant connections in our clients' customer base. It has a straightforward API that pulls data from a customer's database and builds a map of the connections within.

Ravelin Connect can be used during investigations to discover, identify and confirm suspicious behaviour including account takeover attacks. You can surface and discover suspicious networks by size, velocity or connectedness of key entities such as device. This means you can instantly see if one or several devices are accessing accounts they shouldn't be.



What Ravelin does to stop ATO

Ravelin has introduced a number of different ways to combat ATO. Given the different actors, motivations and techniques at play as well as the ever changing nature of criminal behaviour, it is important to have an adaptable and multifaceted approach to tackle ATO effectively.

Breached credentials

Ravelin maintains a breached credentials database. You can make calls to this database at login, during registration or password update to verify if we've seen the credentials in the wild.

Knowing whether credentials have been compromised allows merchants to take proactive steps to prevent ATO attacks before they happen, protecting your customers accounts and your company from the fallout of an attack.

You can also search for and view users that have logged in with credentials that appear in our database - providing additional context during investigations.

Rate limits

We have added customizable rate limits that specifically target ATO at login around device, username and IP. Thresholds can be set for this depending on your specific operational requirements. Rate limits are useful for tackling high volume attacks.

In addition, we check for things we know can indicate that a user is a fraudster like proxies and TOR.

Having rate limits in place at login that target behaviour associated with ATO helps to ensure that merchants can stop attacks at the door.

Rules

We can set ATO specific rules around device, username, IP and velocity. For example, if the same device tries to access X accounts within a set time frame it will be blocked. Rules like this are especially useful for tackling 'low and slow' volume attacks. This can help to protect good customer accounts from more strategic attacks, protecting your reputation and your bottom line.

Material account changes

Informing a user of material changes to their account or behaviour can be a simple way of mitigating the risk of ATO and ensuring that any attacks are dealt with quickly.

We detect and inform you if:

- A new device accesses the account
- A new login location is detected
- A new browser is detected
- A password is changed
- A new email is added
- A new phone number is added
- A new billing address is added
- A new delivery address is added
- If we detect suspicious activity on the account

You can then decide if you would like to notify the user via text or email that a change has been detected and request that the customer confirm the behaviour was legitimate.

Collecting and surfacing login activity data

We provide oversight of login activity within our dashboard. Login activity reporting is available to explore via our Analytics tool, making it easier to spot anomalies in 'normal' login activity across your customer base. In addition, you can interact with this data via a filterable login list and drill down to view relevant information for a specific customer on their customer profile.

Combining data from login with other data we get on customer identity and behaviour such as orders, payment methods, transactions and locations we can provide a much wider context for understanding if a customer has been a victim of ATO.

Model behaviour

As we develop data on the behaviour and actions taken by fraudsters it is possible to work with a client to develop machine learning models that target ATO. This approach has huge potential for detecting anomalies and uncovering hidden patterns in the fraudsters' attack strategies.

Conclusion

Account takeover is a single term for a variety of different threats that are faced by every online business. Each account is vulnerable in some way and each one is a potential financial and reputational loss to your business if not protected. It is essential for good customers to be able to trust in the security of their online accounts.

The good news is that there are a variety of approaches that can help you to protect your customers and your business. The online industry as a whole has a collective interest in preventing ATO before trust in online businesses is eroded any further.