Account takeover – The tip of the cyberthreat iceberg

MERCHANTS

Data breaches are now a fact of life, exposing ever-growing numbers of account data. This endless stream of records is **fueling credential testing attacks for account takeover** – undermining digital trust and authentication as we know it.

Proactive solutions are vital for merchants to gain control over their environments and detect threats before they emerge.

NuData Security

mastercard

Walking on thin ice

2017 closed with 1,579 data breaches leaving customers' sensitive data exposed. Over **nine billion personal records are floating in the dark web**. The consequences of this surge in stolen credentials are sophisticated and scaled automated credential testing attacks that take over accounts. Inexpensive and automated credential testing tools are making it easier and cheaper for fraudsters to check the validity of hundreds or thousands of username/password combinations in mere moments.

What this means for your business

The ripple effect of stolen credentials is dangerous to both consumers and enterprises due to the increasing impact of credential testing and resulting account takeover.

According to NuData's analysts, account takeover (ATO) has increased tenfold in 2017, representing up to 50% of some retailers' web traffic (and sometimes more for higher value accounts or during peak seasons). **Credential testing is a key strategy used to pave the way for an ATO**: it verifies stolen credentials en masse before launching the attack that will directly impact your customers' experience, and your bottom line.

> ***"Credential testing and other types of mass-scale attacks that lead to ATO are often missed by companies."***
> Shirley Inscoe, Aite Group

Why are other solutions not cutting it?

They miss pre-ATO threats

Most solutions look for fraudulent purchases, addressing nothing but the tip of the iceberg. They are missing the key threat vector – where accounts are tested by mass-scale attacks and becoming more sophisticated and impactful every day. These business-threatening attacks happen well before the account takeover occurs days, weeks or even months before you see a fraudulent transaction.

NuData Security
mastercard

The ATO iceberg

What you see

ATO above the surface

Account takeover

This is the last step in the ATO-attack chain, and it's also the only time most e- and mCommerce companies realize that they have a problem. At this stage, bad actors access the accounts and leave you with:

- Fraudulent purchases
- Increased chargebacks
- Reward abuse
- Customer churn

9 minutes

The time it takes for stolen data to be sold on the dark web, and then used by a criminal to commit cybercrime

What you don't see

ATO below the surface

Automated attacks

The bad actor uses automated scripts to test the stolen credentials against merchant login interfaces to find the working ones.

Using 'online validation aggregators' the bad actor keeps testing the same credentials, even hourly, to make sure they are still valid – until someone buys them for account takeover fraud.

Some of these attacks are:

- Credential testing
- Credential harvesting
- Brute-force attacks
- Credential stuffing

NuData Security

mastercard

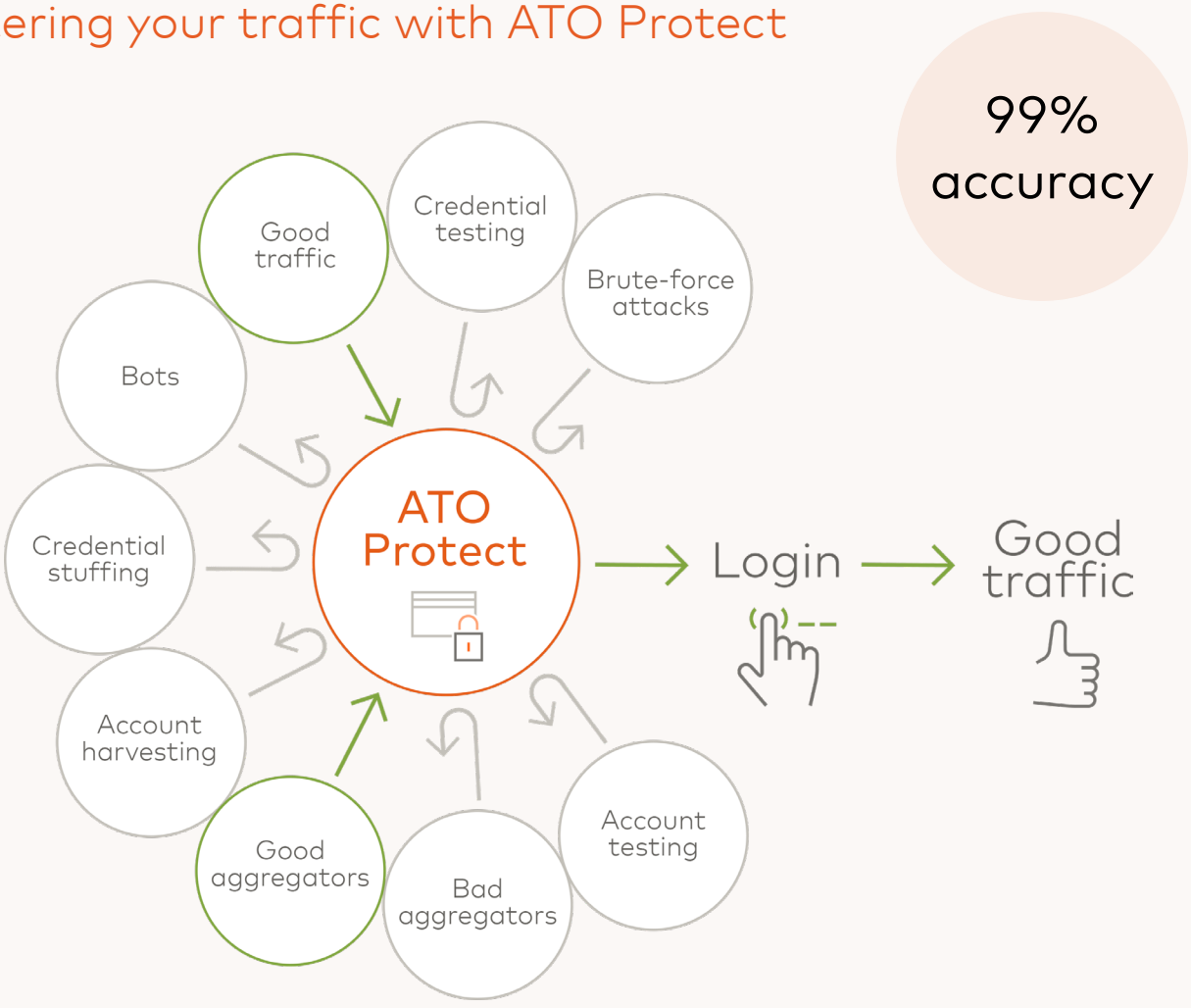
ATO Protect by NuData

Stop ATO before it starts

Our exclusive solution for credential testing and ATO protection shields merchants against the stages of this automated fraud scheme with **99% accuracy**.

We use cutting-edge technology such as behavioral analytics, device and connection detection, and machine learning. Our multi-layered solution accurately identifies if the user behind a login attempt is legitimate or a script part of a mass-scale attack.

Filtering your traffic with ATO Protect



NuData Security
mastercard

ATO Protect allows you to

Expose account takeover

Block any fraudulent automated activity in real time before it can access your authenticated environment, without blocking or adding friction to your good users.

Monitor your traffic

Look at patterns, trends, types of browsers, custom device settings, and hundreds of additional data points from the population and down to the individual level. Credential-testing attacks create subtle changes that can be easily recognized with ATO Protect.

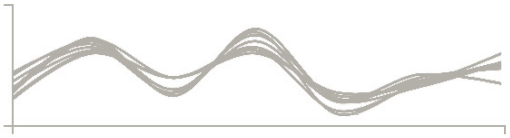
Analyze the device intelligence

With enhanced device intelligence, you can look at the device, location, and connection to analyze your traffic. Monitor the information coming from the device and find out if it is spoofed, in real time.

Learn from your attackers

Leverage dynamic tools to understand the attacks, their techniques, and learn from them to protect you from future evolved attacks. Machine learning technology keeps you ahead of the fraud curve by stopping automation that attempts to pose as a human.

Sample profile of account user



Sample profile of a simple bot

Sample profile of a sophisticated bot

Our proven track record

A U.S. multi-brand online merchant with major automated account takeover problem:

Their solution was letting fraud through. ATO Protect immediately caught all the threats before the login.

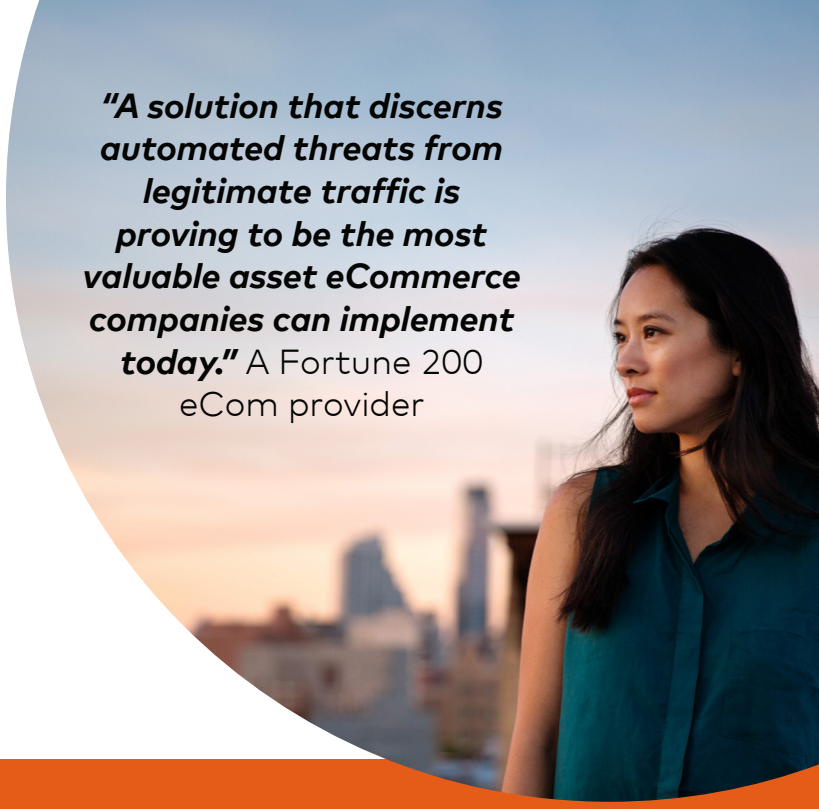
- Over 10,000 credential testing attacks blocked per day.

NuData Security

mastercard

Turn on ATO Protect to

- Identify automated account takeover and credential testing attacks with **99.9% accuracy**
- Protect your environment at the **pre-authentication** stage
- End **automated** threats
- Dynamically adapt to **ever-evolving**, sophisticated attacks



"A solution that discerns automated threats from legitimate traffic is proving to be the most valuable asset eCommerce companies can implement today." A Fortune 200 eCom provider

To learn more, visit **www.nudatasecurity.com/ato-protect**
Email us at bizdev@nudatasecurity.com
or talk to your Mastercard representative.

About NuData

We are an award-winning Mastercard company that offers **ATO Protect**: An enhanced pre-authentication security solution that blocks account takeover and credential testing attacks.

Our unique solution uses cutting-edge multi-layered technology such as behavioral analytics, device and connection intelligence, passive biometrics and a real-time trust consortium to accurately identify who or what is accessing your environment with near 100% accuracy.

We are trusted by major global brands to secure their environment from sophisticated, mass-scale automated ATO attacks and protect the digital space.

NuData Security
mastercard