Make Risk Less Risky: How to Foil the Fraudsters

Leverage a ML-driven decisioning engine to protect your customers from account attacks.

> **Consumers are doing more of their day-to-day tasks online than ever. They bank. Shop. Work. Update social feeds. Network with friends and colleagues. Watch cat videos.**

The number of online accounts people have to manage today has skyrocketed, particularly over the last decade. Industry estimates vary widely, but it's safe to say that an average adult consumer has anywhere from dozens to more than a hundred online accounts that require a username and password.

That's a lot to manage—and the stark reality is that most of us don't do it very well. We reuse passwords across multiple accounts or create easy-to-remember passwords like 123456 (shockingly, still the number one most commonly used password in the world). One study by **LogMeIn** found that corporate employees reused a password an average of 13 times. And while 91% of survey respondents said they know reusing passwords is a major security risk, 66% still "mostly" or "always" use the same password.

These weak, overused passwords are low-hanging fruit for hackers, and an easy entry point into a whole lot of personal and financial data, such as email addresses, credit card numbers, and social security numbers, that could net fraudsters loads of cash on the dark web. Cybercriminals also use stolen credentials to take over legitimate accounts, which can wreak mighty havoc in anyone's life.

WHAT IS ACCOUNT TAKEOVER, EXACTLY?

Account takeover, or ATO, occurs when a hacker accesses an existing online account using stolen credentials. Once the cybercriminal gets into the account, they take control of it by changing the password or other account information, thereby locking the true user out. Now they can do whatever they want depending on the account type, such as steal proprietary information, withdraw funds, make unauthorized purchases, commit credit card fraud, and much more.

The underlying motivation for ATO is primarily financial gain through the theft of money or information. ATO fraud is a serious threat to a wide variety of accounts, including checking and savings accounts, credit cards, government benefits accounts, social media accounts, e-commerce accounts, and store loyalty accounts. The more we do online, such as using applications for digital payments, stock market investing, and cryptocurrency trading, the more potential vulnerabilities we present to fraudsters.

Types of accounts vulnerable to ATO:

- ✓ Checking accounts
- ✓ Savings accounts
- ✓ Investment accounts
- ✓ Credit cards
- ✓ Government benefits accounts
- ✓ Social media accounts
- ✓ E-commerce accounts
- ✓ Store loyalty accounts

While ATO isn't a new phenomenon, the frequency of attacks has recently skyrocketed. More than **one in five U.S. adults** (22%) has been a victim of ATO—which equals over 24 million households. Industry experts estimate **$11.4 billion in total losses** due to ATO in 2021, a 90% increase from 2020. One recent article in **Forbes** even referred to it as the "ATO epidemic."

While fraudsters traditionally targeted financial institutions for ATO (and still do), today all kinds of organizations—such as hospitals, universities, insurance companies, and online retailers—are at risk. Any organization that requires a username and password is vulnerable, as personal information is ultra-valuable. Personally identifiable information (PII) enables cybercriminals to create chaos for a customer, from opening lines of credit to filing fraudulent insurance claims to applying for government benefits. Fraudsters also use PII in phishing and spamming activities to appear more convincing to victims.

THE MANY WAYS FRAUDSTERS GAIN ACCESS TO CREDENTIALS

There are many ways fraudsters can find legitimate usernames and passwords:

- **Data breaches** - also on the rise, data breaches are a good source of stolen credentials.
- **Brute force attacks** – some cybercriminals use bots that can test out many different combinations of letters, numbers, and special characters very quickly to crack an account. In fact, some of those bots can figure out an 8-character password in less than an hour.

How ATO works: the devious design

Cybercriminals steal valuable account information and sell it on the dark web

↓

Fraudsters purchase stolen data and use bots that test credentials and attempt to log in to a wide range of online sites

↓

Some credentials are eventually verified and either sold to other criminals or used for ATO

↓

Fraudsters make unauthorized changes to the account, making it difficult (or even impossible) for the account owner to regain control

Even in cases where the owner regains access, it is often achieved at high financial cost and/or a damaged relationship with the business

- **Credential stuffing** – with the knowledge that people tend to reuse usernames and passwords across multiple accounts, credential stuffing uses bots and automated scripts to try and get into accounts.
- **Phishing** – these scams, which can be transmitted via text message, live phone calls, email, fake websites, and live chat sessions, trick people into giving out their credentials.
- **Viruses or malware** – these malicious programs can be uploaded to a user's device without their knowledge, where they'll steal private information by logging keystrokes or other methods.
- **Man-in-the-middle attacks** – transmitting information over unsecure networks could leave a user's credentials vulnerable to interception by cybercriminals. Public Wi-Fi networks and residential internet routers are common culprits for this type of attack.
- **SIM card swapping** – mobile phone providers will swap out a SIM card when someone buys a new device. A fraudster can hack this legitimate service by impersonating the customer and convincing the mobile provider to port the customer's phone number to a new SIM card. Now the fraudster can activate the customer's banking app, for instance, on their phone and access their account.
- **Mobile banking trojans** – cybercriminals create a fake webpage that overlays a bank's legitimate website. Account credentials are then captured when a customer logs in, and fraudsters can alter transaction information—such as redirecting a funds transfer. How to Detect ATO

HOW TO DETECT ATO

It can be really tough to detect ATO attacks because most fraudsters are invested in staying under the radar and won't try to make themselves known. The longer they can control the account, the more they can ultimately gain. The point is to subtly change account information so the account owner won't be notified of any problems.

There are a few signs that could point to ATO if you know what to look for. A large number of unsuccessful login attempts, for instance. That's why some organizations lock users out after failed login attempts. Other signs include excessive password resets, successful logins from unfamiliar or suspicious IP addresses, login attempts from irregular geographic regions, a sudden flurry of account detail changes across multiple accounts, account activity on "unknown" devices (which could point to device spoofing), logins to multiple accounts from a single device, and multiple accounts using the same details (email address or phone number, for instance).

Some of the best ways to detect ATO or identify warning signs before t even happens is to have a system that enables continuous monitoring. Organizations should have full visibility into every user's actions at all times. With comprehensive monitoring, it's possible to prevent ATO because a fraudster has to do a few things in the account before they can actually steal money—like entering a new payee or changing a mailing address.

Today's organizations can't afford to sit by and do nothing—so that's where ATO prevention solutions come in.

Ultimately, detecting and eliminating ATO attacks can be a real challenge because it's primarily caused by customers who are unaware of or resistant to the need for strong, unique passwords. Short of creating mandatory rules for password creation, there's little an organization can do to control customer choices.

The practices of ATO are constantly evolving. Cybercriminals are developing new tools and processes to improve their takeover abilities all the time. In fact, ATO is evolving so fast that trying to respond after a takeover is almost like doing absolutely nothing.

Today's organizations can't afford to sit by and do nothing—so that's where ATO prevention solutions come in.

ATO PREVENTION SOLUTIONS: WHAT TO LOOK FOR

Many solutions are available today that help protect organizations from ATO attacks and other fraud. When choosing a vendor for ATO prevention, there are a few must-have features and capabilities. Continuous monitoring, mentioned above, is a biggie. Organizations need that constant visibility into user activity.

A good solution will also be designed to identify patterns and alert organizations to anomalous user behavior and activity. It should be able to detect bot attacks and allow the creation of granular rules or policies that help automatically assess risk based on multiple data points. And it should have the capability to automatically request the customer for more information, such as a fingerprint or one-time code.

The most effective ATO solutions will also:

- Be easy to use, deploy, and manage
- Offer rapid response to threats
- Provide intelligent automation built on real-time insights
- Reduce customer friction
- Enable access to lists of known exposed credentials to compare with the organization's user accounts
- Offer comprehensive reporting capabilities
- Deliver excellent technical support and consultation when needed

HOW PI CAN HELP

Pi gives organizations the tools and capabilities they need to stop ATO attacks and more effectively manage risk. The platform is a smart decisioning engine driven by machine learning (ML) that serves as a fraud prevention layer for enterprises.

With Pi, your organization can create dynamic risk scores and tiered experiences for each user based on their profile. The system flags unusual behavior, turning binary risk decisions into controlled growth opportunities. We do this through intelligent decisioning—scoring each user through first and third party data sources before tailoring unique services and solutions to each user. The result is a highly responsive risk management platform that creates frictionless experiences for your users. Meanwhile, we dynamically monitor user activity to auto-adjust risk scores, rules, and thresholds throughout the entire customer lifecycle.

In addition to helping prevent ATO, Pi can also help detect and prevent onboarding fraud, transaction fraud, promotional and marketing fraud, and collusion fraud. It can assess merchant and consumer risk and help in anti-money laundering (AML) initiatives.

The Three Ds of ATO Prevention

DETECT

Tailor experiences through intelligent risk tiering

DIAGNOSE

Dynamically monitor activity and pinpoint vulnerabilities

DEPLOY

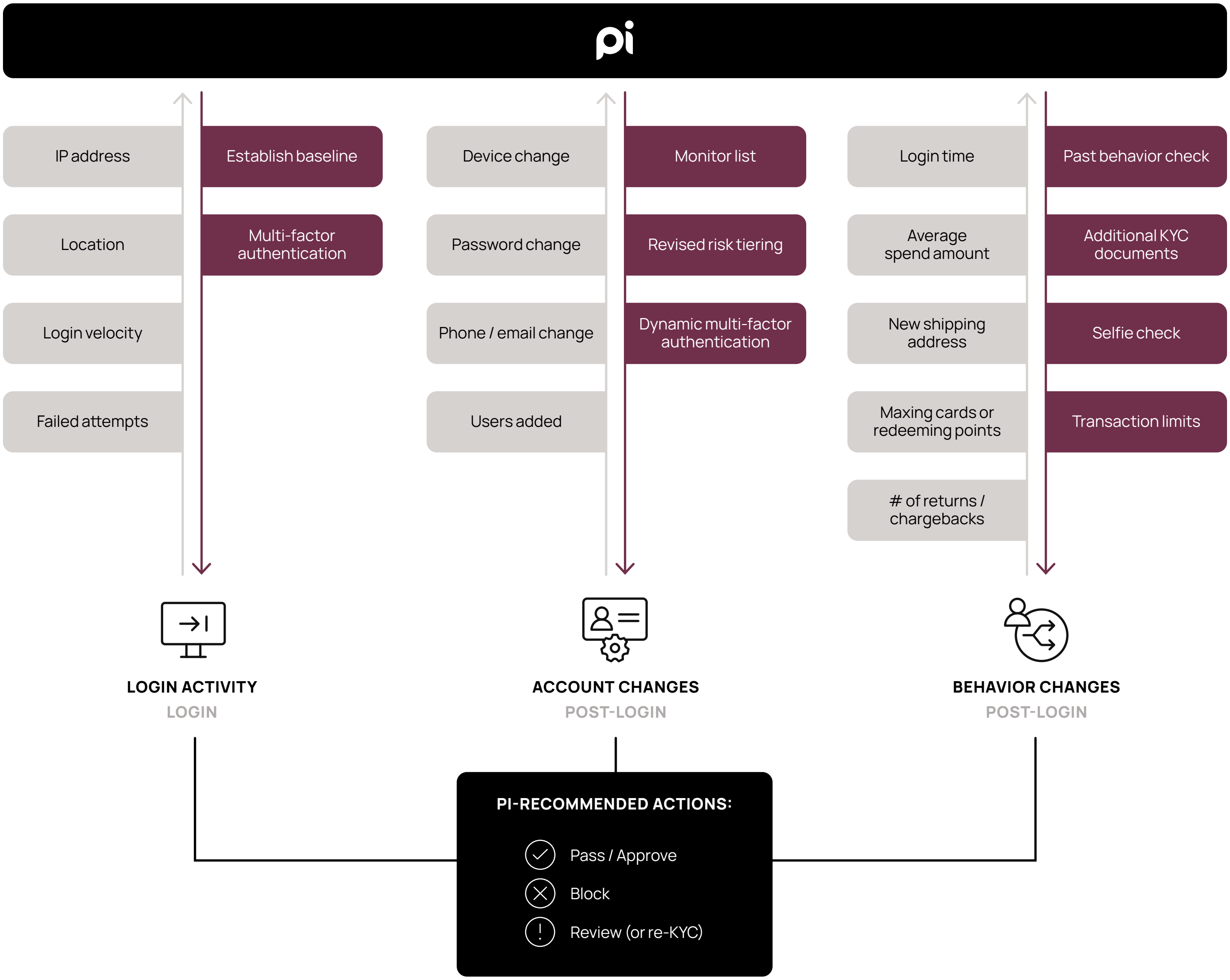
Connect data sources and configure rules and policies

Pi highlights:

50 milliseconds AVERAGE DECISIONING TIME

3-4 weeks IMPLEMENTATION TIME

2x faster DECISION MAKING THAN THE INDUSTRY AVERAGE



pi

IP address — Establish baseline
Location — Multi-factor authentication
Login velocity
Failed attempts

LOGIN ACTIVITY
LOGIN

Device change — Monitor list
Password change — Revised risk tiering
Phone / email change — Dynamic multi-factor authentication
Users added

ACCOUNT CHANGES
POST-LOGIN

Login time — Past behavior check
Average spend amount — Additional KYC documents
New shipping address — Selfie check
Maxing cards or redeeming points — Transaction limits
# of returns / chargebacks

BEHAVIOR CHANGES
POST-LOGIN

PI-RECOMMENDED ACTIONS:

- ✓ Pass / Approve
- ✕ Block
- ! Review (or re-KYC)

What makes us different from the other guys:

- Data ingestion
- Dynamic risk tiering
- Anomaly detection
- No-code rule builder
- Smart rule simulations
- Machine learning (ML) studio

As life and work get increasingly digital, online fraud and ATO attacks are pretty inevitable. Data gets breached. Credentials get stolen. But that doesn't mean you are at the mercy of fraudsters. With the right tools and technology, your organization can reduce the risk of ATO through more powerful protection of your customers' accounts.

Every day, Pi:

- ✓ Evaluates 5+ billion rules
- ✓ Makes 427 million decisions
- ✓ Ingests 1.8 billion records

Stop account takeovers with Pi

To learn more about how Pi can protect your business and customers from ATO, schedule a demo at pi@paytm.com. For more information on Pi visit **pi.paytm.com**.