SpyCloud

CASE STUDY

How a **global retailer** stops **identity-based attacks** before authentication

PROTECTING CONSUMER IDENTITIES with
SpyCloud + PingOne Advanced Identity Cloud »

Millions of consumer accounts. Over 2,000 retail locations. One modernized identity infrastructure. This Fortune 500 global retailer deployed PingOne Advanced Identity Cloud (AIC) with SpyCloud Consumer Threat Protection embedded into every authentication journey – delivering continuous credential exposure detection, advanced bot protection, and automated fraud prevention at scale.

CONSUMER ATO AND FRAUD PREVENTION AT THE POINT-OF-AUTHENTICATION

For a large-scale retailer operating millions of consumer accounts across e-commerce and business commerce platforms, the threat of ATO, automated bot attacks, and consumer fraud is constant. Attackers don't need to breach systems directly when they can simply purchase stolen credentials from criminal markets and log in, posing as a legitimate user.

Billions of those credentials, harvested from breaches, infostealer malware infections, and successful phishes, are continuously cycled through automated login tools targeting consumer accounts. If an attacker were to gain access, they could commit fraud, make unauthorized purchases with stored payment methods, and exploit saved account data before the account owner even notices.

With consumer trust, checkout conversion, and brand reputation on the line, the retailer needed an identity security strategy that could operate at the speed of its consumer authentication flows to catch exposed credentials and stop fraud before login, not after the damage was done.

THE CHALLENGE

The retailer's legacy customer identity & access management (CIAM) platform lacked standards-based authentication and had no visibility into whether presented credentials had already been stolen. With a high-volume consumer platform that processes millions of transactions, the threat of credential-based fraud, automated bot attacks, and account takeover (ATO) was constant – and growing. Faced with expanding maintenance overhead and stringent performance requirements, the status quo was unsustainable.

THE SOLUTION

The retailer deployed PingOne AIC with SpyCloud Auth Node embedded into consumer journeys, driving continuous credential exposure checks and automated, risk-proportionate remediation at every identity event. The deployment was supported by Optiv, whose strategic alignment with key stakeholders helped accelerate the evaluation process and close.

SpyCloud

CASE STUDY

HOW IT ALL WORKS

SpyCloud infiltrates criminal communities directly, recapturing stolen identity data and adding it to our data lake weeks to months before it surfaces in criminal underground forums.

In this deployment, the SpyCloud Auth Node plugs directly into the no-code orchestration layer of PingOne AIC. At any point in the consumer authentication journey – account creation, login, or credential update – the SpyCloud Auth Node performs a continuous check of the authenticating credential against SpyCloud's ever-growing database of recaptured identity data from the criminal underground, spanning breaches, malware logs, combolists, and phished data.

Based on the result of the credential query, the journey routes automatically to a configurable, risk-proportionate action:

- **Mandatory password reset when an exposed credential is detected at login**
- **Blocking of new account creation or credential updates using known exposed passwords**
- **Step-up MFA enforcement for moderate-risk matches, adding a friction layer precisely where fraud risk is elevated**
- **Dynamic prompts guiding users toward creating stronger, unexposed credentials**

By the time most security tools see exposed consumer data, attackers have already used it to commit fraud. The SpyCloud Auth Node closes the gap – stopping identity-based fraud at the door rather than detecting it in a transaction log.

THE RESULTS

The retail customer now benefits from continuous detection and automated remediation of exposed credentials at customer login, account creation, and password reset – protecting millions of consumer accounts from ATO and fraud without adding friction for legitimate users.

BEHAVIORAL FRAUD TOOLS DETECT ANOMALIES *AFTER* AN ATTACKER IS ALREADY INSIDE.

SPYCLOUD STOPS THE USE OF EXPOSED CREDENTIALS *BEFORE* AUTHENTICATION, CUTTING OFF THE FRAUD BEFORE IT STARTS.

SpyCloud

CASE STUDY

RESULTS

CONSUMER ATO & FRAUD PREVENTION

SpyCloud provides the exposure intelligence the Ping platform needs to detect and respond to exposed credentials at the moment of authentication, without manual intervention or delays. Consumer accounts are protected across account creation, login, and password reset touchpoints – eliminating the entry point for identity-based fraud that follows a successful account takeover.

EXPOSURE-AWARE CONSUMER IDENTITY JOURNEYS

SpyCloud's identity intelligence enriches PingOne AIC to deliver consistent, secure login and account creation experiences, improving both the organizational security posture and consumer trust. When consumers know their accounts are protected from fraud, brand loyalty follows.

RISK-PROPORTIONATE, AUTOMATIC REMEDIATION

Step-up MFA and forced password resets apply only when real exposure threats are confirmed with SpyCloud data, keeping the user experience smooth for legitimate users while creating a hardened defense against identity-based attacks and the fraud they enable.

KEY OUTCOMES

- **Protects millions of consumer accounts from ATO and fraud at the point of authentication**
- **Eliminates the primary entry point for consumer fraud by blocking exposed credentials before access is granted**
- **Eliminates manual breach monitoring with continuous credential exposure detection and automatic remediation response**
- **Applies friction only when real risk is confirmed, preserving conversion rates and user experience for legitimate consumers**

*"SpyCloud has spent years building **the most comprehensive database of recaptured darknet data in the industry**. Partnering with Ping Identity means that **intelligence is actionable at the exact moment of authentication – for both workforce and consumer identities**. That's a meaningful shift from reactive breach response to proactive, continuous identity protection for this customer."*

DAMON FLEURY | CHIEF PRODUCT OFFICER, SPYCLOUD

ORGANIZATION-WIDE VALUE

The value of the SpyCloud and Ping Identity AIC integration extends beyond consumer-facing authentication. The same intelligence and enforcement capabilities that protect consumer accounts also feed into the retailer's broader fraud prevention and security posture, including workflows that inform the fraud team, support SOC investigations, and provide a shared signal layer between identity, security, and product teams.

SpyCloud data gives identity and fraud teams exposure context that traditional security tools don't surface. That means fraud teams receive pre-authentication signals rather than post-authentication alerts – shifting the response from reactive investigation to proactive prevention. By protecting consumer accounts from ATO and fraud, the identity security investment directly supports the retailer's brand reputation by making sure that millions of consumers transacting across its digital channels can trust their accounts are secure.

NEXT STEPS

Start building your **SpyCloud x PingOne** AIC Integration

Explore more **SpyCloud x PingOne**

Learn about **SpyCloud Consumer Threat Protection**