

National Grocery Chain Protects Against Account Takeovers

Manually monitoring for stolen credentials is incredibly time consuming and ineffective. Sometimes months can go by before security teams detect leaked information. Also, threat actors can publish then remove information between searches, adding another layer of difficulty tracking this down. The time lag creates an advantage for cybercriminals.

With Flare's automated Threat Exposure Management solution, the grocery chain simplified tracking down stolen credentials from their loyalty program eCommerce platform. This shifted their cyber strategy from reactive to proactive: from addressing account takeovers to flagging stolen accounts and addressing the issue before threat actors could abuse the stolen credentials.

By monitoring high-risk external threats with Flare, the national grocery chain not only monitored and stopped those threats, but also accelerated their mitigation efforts.

Challenge: Threat Actors Target Loyalty Programs

The grocery chain's security team investigated threat actors targeting the online grocery retail platform accounts for account takeovers. Malicious actors publish threats, hacks, and stolen data across hundreds of illicit sources, which makes manual monitoring too time-consuming. Threat actors target loyalty program accounts often found in retail, hospitality, and travel industries because:

The Customer

-  Over \$15B in revenue each year
-  Almost 100,000 employees
-  Offer popular online grocery retail platform, a loyalty program, and pharmacy services

“Before Flare we struggled to catch up to threat actors causing damage after finding customers' leaked credentials. With Flare's Threat Exposure Management (TEM) platform we're staying on top of stolen accounts with automated monitoring and preventing fraud from happening in the first place.”

**-CTI Director
National Grocery Chain**

- They typically do not have 2FA/MFA
- They are not perceived as accounts that need a lot of protection like a banking account, even if they include payment information

The customer's security team searched for solutions that would reduce account takeovers and protect the brand reputation while increasing customer retention and loyalty.

Benefits: Security Team Secures Stolen Accounts Before Threat Actors Abuse Them

With Flare, the grocery chain regained their customers' trust by drastically decreasing account takeovers. The security team could find stolen accounts and secure them before threat actors gained access through credential stuffing.

By searching through billions of compromised credentials through Flare's database, the customer's security team conducted their searches in one place as opposed to combing through hundreds of illicit attacks.

Their adapted mitigation strategy with Flare has significantly reduced account takeovers and fraud.

Gartner
Peer Insights.

4.9 ★★★★★

AICPA
SOC 2
TYPE II
Thozopass™

[Sign Up for a Free Trial →](#)



flare.io

hello@flare.io