HackNotice

Proactively Detecting Consumer Credential Exposure to Prevent Fraud

Success Stories in Retail and Financial Services

CASE STUDY

Introduction

As customer data continues to flood the dark web, organizations in both retail and finance are struggling to protect accounts from credential reuse and takeover. HackNotice's Research service offers an advanced, no-input-needed approach to identifying leaked consumer credentials in real time—enabling organizations to reset credentials and block fraud before damage occurs.

For three forward-thinking companies—a large restaurant chain, a regional credit union, and a regional bank—HackNotice has become a frontline defense in minimizing customer account takeovers and unauthorized access.

The Challenge

With large customer bases and high-value targets, these organizations faced a shared threat: exposed customer credentials were fueling fraudulent purchases, unauthorized account activity, and reputational damage.

A **Fortune 500 restaurant chain** needed to detect exposed logins tied to their loyalty and payment portals to prevent fraudulent orders and gift card abuse.

A **regional credit union** sought a way to spot leaked consumer banking credentials to proactively prevent fraudulent transfers and account takeovers.

A **regional bank** was looking to reduce alert fatigue by only surfacing high-risk, high-confidence credential leaks relevant to their platforms.

Each organization required a solution that could scale across millions of potential users, **without requiring PII as an input**, and that could filter out low-complexity noise for more actionable alerts.

Solution

HackNotice's **Research** service delivered targeted dark web monitoring based on each customer's domain and login URLs—without the need to upload or store any consumer data.

Credential Exposure Detection at Scale

HackNotice detected when credentials tied to the customer's login URLs or brand appeared on the dark web, surfacing only verified, high-confidence records.

No Customer Data Required

The system uses the client's domain, login URLs, and other digital identifiers to detect leaked credentials—eliminating the need for customer data sharing while maintaining coverage.

Minimum Password Complexity Filtering

To reduce false positives and noise, HackNotice applied a password complexity threshold—ensuring that only records meeting specific security criteria generated alerts.

Proactive Remediation

With every alert, security teams were able to reset credentials, notify affected customers, and take steps to block suspicious logins before attackers could act.

Results

A Cybersecurity Engineer at a Fortune 500 restaurant chain highlighted that HackNotice delivers automated, high-confidence alerts tied to exposed customer credentials—supporting a faster fraud mitigation workflow.

A CISO at a regional credit union acknowledged that HackNotice provided multiple timely alerts related to both employees and customers, significantly boosting the team's response capabilities.

A VP of InfoSec at a regional bank said HackNotice offered early visibility into fraud activity while keeping alert volume manageable—helping the team act quickly without alert fatigue.

Multiple Actionable Alerts per Month

Each customer receives several high-confidence alerts every month, allowing them to proactively secure affected customer accounts.

Reduced Fraud and Customer Risk

By detecting and addressing credential leaks early, these organizations significantly reduced instances of fraud, chargebacks, and customer account compromise.

Efficient, Scalable Consumer Monitoring

HackNotice enabled scalable credential exposure monitoring across millions of consumers without requiring sensitive customer data—ensuring privacy and speed.

About HackNotice

HackNotice is the leader in dark web intelligence and breach monitoring, helping organizations around the world reduce risk from credential exposure, data leaks, and supply chain threats. Our platform continuously monitors the global dark web—including criminal forums, Telegram, marketplaces, and breach archives—for stolen credentials, infostealer logs, and leaked corporate data.

HackNotice provides real-time alerts for ransomware events, data breaches, and account exposures, empowering security teams to take immediate action. From individual employee protection to comprehensive vendor monitoring, we help enterprises detect and mitigate risk before it becomes a compromise.

Our services include:

Credential and Session Exposure Monitoring
Discover when your employees, customers, or systems appear in infostealer logs or breach dumps.

Third Party and Supply Chain Risk Intelligence
Track vendors and partners for breaches, ransomware attacks, or data leaks that may put your business at risk.

Ransomware & Data Breach Alerts
Get real-time, actionable notifications about new attacks across your ecosystem.

Dark Web Incident Analysis
Receive deep-dive investigations into specific dark web data incidents, including attribution, scope, and remediation guidance.

With HackNotice, your team gains early visibility into attacker data and behavior—enabling you to respond quickly, protect identities, and minimize business disruption. Learn more at hacknotice.com or contact us to schedule a tailored threat briefing.