FLASHPOINT

# Compromised Credentials Monitoring: Customer

Organizations need to protect their customer base and have insight into whether data has been compromised. Compromised Credentials Monitoring - Customer allows organizations to monitor for compromised customer credentials, while enabling enterprises to prevent fraudulent activity and protect their client base.

## Key Benefits

- Analyze the exposure of customers and proactively take action to prevent fraud or misuse on company-owned platforms
- Ability to protect customers without compromising proprietary customer credentials via secure hashing
- Access via Webhook: Receive push notifications when a customer has been compromised, enabling teams to take a proactive approach of protecting client accounts against fraudulent activity
- Actively prevent misuse, which could lead to large-scale incidents and brand reputational damage
- Flashpoint's secure hashing technology enables safe transfer of credentials without exposing sensitive customer information

## Use Case

### FRAUD LOSS AVOIDANCE

Threat actors obtain stolen or leaked credentials and have sophisticated credential stuffing measures to access multiple accounts and websites where the stolen passwords may have been reused. Companies should take action on compromised accounts where passwords were reused to mitigate risk of fraud loss from their accounts.

- **RESET CUSTOMER PASSWORDS; MONITOR AND FLAG COMPROMISED ACCOUNTS**
  Organizations may use Flashpoint's Compromised Credentials Monitoring - Customer data to inform policy decisions about whether to automate a password-reset process, monitor and flag an account, or notify a customer about their exposure. Flashpoint's secure partial hashing capability ensures that an organization's customer is protected; hashing ensures compromised credential information may be securely transferred between Flashpoint and a customer.
- **REQUIRE STRONG UNIQUE PASSWORDS FOR NEW ACCOUNTS**
  Organizations can require customers creating accounts to use passwords that have not been compromised previously. If a username-password combination is found within Flashpoint's Compromised Credentials dataset, the organization can prompt the user to choose a different password.

## ABOUT FLASHPOINT

Trusted by governments, global commercial companies, and educational institutions, Flashpoint helps organizations protect their most critical assets, infrastructure, and stakeholders from security risks such as cyber threats, ransomware, fraud, physical threats, and more. Leading security practitioners—including cyber threat intelligence (CTI), vulnerability management, DevSecOps and vendor risk management teams—rely on the Flashpoint Intelligence Platform to proactively identify and mitigate risk and stay ahead of the evolving threat landscape.

For more information, visit flashpoint.io or follow us on Twitter at @FlashpointIntel