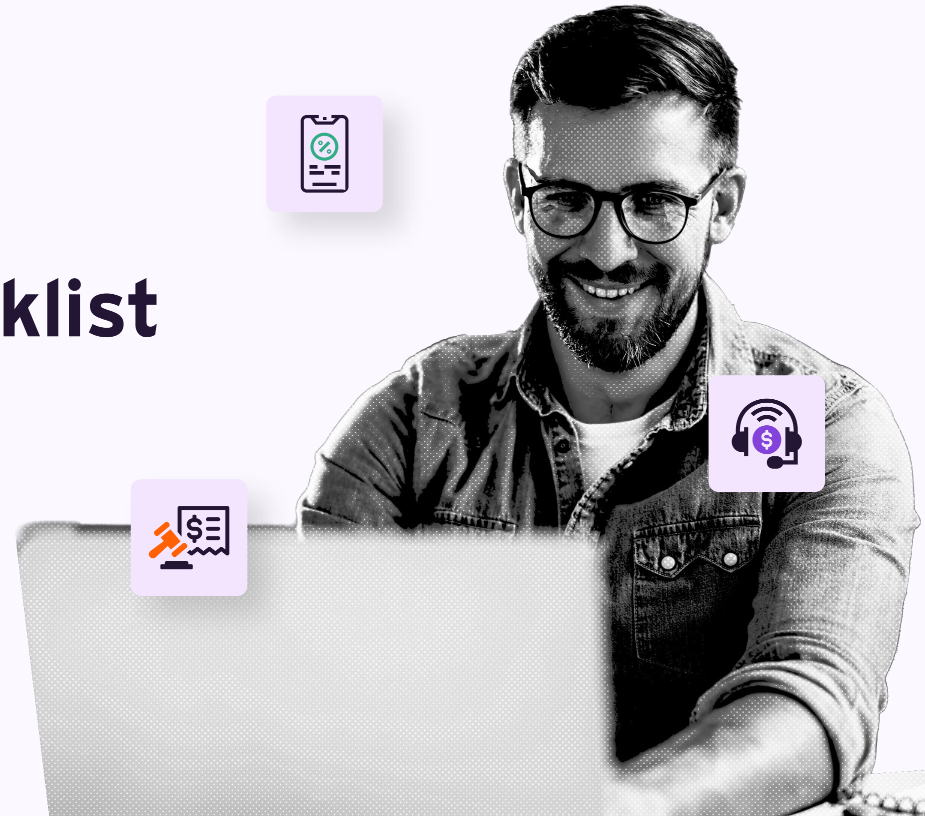
strivacity

Loyalty Fraud Prevention Checklist

Secure your loyalty program without compromising customer experience



Use this checklist to assess your current defenses against loyalty fraud and identify areas where you can increase your protection.

1 Sign-up

Prevent fraudulent accounts and bot attacks from the outset:

- □ **Email and phone number verification:** Ensure contact information is authentic and reachable.
- □ **CAPTCHA or bot detection enabled:** Block automated account creation attempts from known bot networks.
- □ **Identity fraud detection:** Prevent fraudulent sign-ups using temporary or throwaway contact details such as email, phone number, name, and physical address information using known identity fraud and risk signals.
- □ **Phone number fraud detection:** Verify against risky phone numbers such as non-fixed VoIP, detect SIM-swap fraud, and match PII against phone carrier records.
- □ **Geolocation detection:** Compare the user's location to their historical patterns and detect attempts from countries or regions that don't match past behavior or may be linked to fraud.

2 Sign-in

Protect against account takeovers with adaptive security measures:

- □ **Passkeys or passwordless login support:** Enhance security and customer convenience.
- □ **Adaptive Multi-factor authentication (MFA):** Require additional verification for account access.
- □ **Known device detection:** Recognizes devices customers have previously used to sign in and allowing frictionless access for safe logins while challenging unknown or suspicious ones.
- □ **Breached password detection:** Block breached passwords during the sign-in or during a password reset.

3

Reward redemption & account actions

Safeguard high-value transactions and sensitive account changes:

- □ **Risk-based authentication for redemptions:** Trigger additional authentication for large or unusual point redemptions.
- □ **Step-up authentication for profile changes:** Require re-authentication when updating critical account information.
- □ **Anonymous proxy / Tor detection:** Step up authentication if a sign-in is associated with known anonymous proxies or Tor exit nodes.
- □ **CRM and loyalty platform integration:** Share risk signals across systems for coordinated responses.

4

Visibility & monitoring

Maintain oversight and quickly address potential fraud:

- □ **Real-time alerts on blocked or suspicious login attempts:** Keep customers informed of immediate threats and suspicious account activity.
- □ **Dashboard with identity-related insights:** Visualize trends and anomalies in user behavior.
- □ **Audit logs for account changes and redemptions:** Track and review critical actions.
- □ **Filtering by device, geo, risk level, or fraud indicators:** Customize views to focus on specific concerns.
- □ **Consent and identity data versioning:** Maintain records of customer consent and identity changes.

5

Pro tips

Enhance your fraud prevention strategy:

- □ **Regularly review and adjust risk signals:** Adapt to emerging fraud patterns.
- □ **Educate customers on account security:** Promote best practices for password management and account protection.
- □ **Cross-reference support issues with fraud analytics:** Identify potential fraud through customer interactions.
- □ **Restrict high-value redemptions for new accounts:** Mitigate risk from recently created profiles.

How secure is your loyalty program?

strivacity

If you've identified gaps in your current setup, Strivacity is here to help. Our solution provides adaptive access controls, real-time fraud detection, identity verification and real-time insights to protect your loyalty initiatives without compromising customer experience.

For more detailed information on Strivacity's capabilities, visit strivacity.com