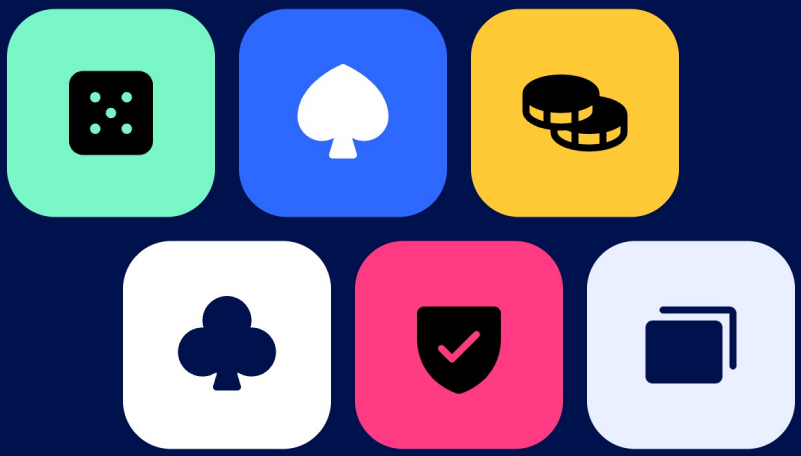
Eight workflow configurations to reduce risk in IGAMING

Eight plays for fraud and risk teams. Each one outlines the threat, what you need in place, how to configure a successful workflow, and what benefits to expect.



0.5%
Average player block rate

60%
Average manual review reduction

<1.3%
Average manual review rate

$45B+
Annual player transaction value secured

© Sift Science, Inc. All rights reserved. Sift and the Sift logo are trademarks or registered trademarks of Sift Science, Inc.

Eight workflow configurations to reduce risk in iGaming

1 Score every deposit

Threat

Stolen cards fund play, then the proceeds are withdrawn.

What you need

A workflow on every deposit event.

How to configure

1. Payment abuse type. Trigger: your deposit event.
2. Route 1: score at or above your block threshold. Action: Block.
3. Route 2: score in the middle. Action: Review Queue.
4. Everything Else: Accept.

Benefit: High-risk deposits stop before play and cash-out. Analysts see only the middle.

2 Check every withdrawal

Threat

Account takeover, then a withdrawal before the real player notices.

What you need

A workflow on every withdrawal event that reads score and account history.

How to configure

1. Payment abuse type. Trigger: your withdrawal event.
2. Route 1: score at or above your block threshold. Action: Block or hold.
3. Route 2: new device plus a withdrawal or payment method change. Action: Review Queue.
4. Everything Else: Accept.

Benefit: High-risk exits get reviewed before funds leave.

3 Add login friction only when needed

Threat

Credential stuffing, phishing, and SIM-swapping put accounts and balances at risk.

What you need

Step-up verification, with Dynamic Friction, for risky logins only.

How to configure

1. Account takeover abuse type. Trigger: your login event.
2. Route 1: unseen device or IP plus a high score. Action: step-up verification (MFA).
3. Route 2: password change after an unfamiliar login. Action: Review Queue.
4. Everything Else: Accept with no added friction.

Benefit: Verification lands where signals warrant it. Legitimate players keep a clean login.

© Sift Science, Inc. All rights reserved. Sift and the Sift logo are trademarks or registered trademarks of Sift Science, Inc.

4 Catch promo abuse at registration

Threat

Fake sign-ups claim welcome offers. 100 accounts on a $50 offer extract $5,000.

What you need

A create account workflow using device and behavioral signals.

How to configure

1. Account abuse type. Trigger: your create account event.
2. Route 1: score at or above your block threshold. Action: Block.
3. Route 2: elevated signals, such as automated behavior or shared devices. Action: Watch, with a webhook that holds promo credit.
4. Everything Else: Accept.

Benefit: Catch the abuser at registration, not after the offer is claimed.

5 Break up multi-account networks

Threat

One person or ring runs many accounts that look independent.

What you need

Links across accounts: shared devices, IP ranges, behavior, and payment methods.

How to configure

1. Create account workflow: send high-risk registrations to Block or a Review Queue.
2. Deposit workflow: send players linked to flagged accounts to a Review Queue.
3. Give reviewers Block, Allow, and request more information.

Benefit: Networks that look clean account by account show up once you link them.

6 Fast-track trusted players

Threat

Over-blocking. Every legitimate player you decline is lost revenue.

What you need

A low-risk route for players with established history, below your fraud routes.

How to configure

1. Build your block and review routes first. Route order decides which one fires.
2. Add a route for a low score plus an established history. Action: Allow.
3. Review monthly. Watch false positives as closely as fraud losses.

Benefit: Low-risk sessions proceed with no added friction. Fewer false declines.

© Sift Science, Inc. All rights reserved. Sift and the Sift logo are trademarks or registered trademarks of Sift Science, Inc.

7 Keep review queues for the gray zone

Threat

Reviewers buried in volume, working cases a workflow could decide.

What you need

Queue routes for the middle of your score range only, with decisions set per queue.

How to configure

1. Name each queue for its job and choose the decisions reviewers can take in it.
2. Route only medium-risk cases to it. Block high scores. Accept low scores.
3. Watch queue volume. If it grows, adjust thresholds or add a route.

Benefit: Sift iGaming customer averages: manual reviews down 60%, manual review rate under 1.3%. Customer averages, not a promise for one workflow.

8 Measure every route, then retune

Threat

A workflow that was right at launch drifts as fraudsters adapt.

What you need

A monthly look at Workflow Metrics and Route Metrics, approvals next to blocks.

How to configure

1. Review Route Metrics. Retire or rewrite routes that rarely fire or fire wrongly.
2. Track approval rate for legitimate new depositors next to block rate. If one improves while the other stalls, retune before adding a rule.
3. Check where abuse clusters: geography, device, payment method, registration time.

Benefit: Smaller rulesets, fewer surprises, and workflows that keep pace with your promotions calendar.

How every play works

Trigger event
Deposit, withdrawal, login, or sign-up

→

Route 1
High risk.
Action: Block

→

Route 2
Middle.
Action: Review Queue

→

Everything Else
No match.
Action: Accept

Routes are checked in order. Only the first match fires. Put your highest-risk checks first.

Workflows decide. AI helps your team see attacks and act on them sooner.

Meet Sift's Fraud Attack Defense Suite →

© Sift Science, Inc. All rights reserved. Sift and the Sift logo are trademarks or registered trademarks of Sift Science, Inc.