How Real-Time Rules Can Stop 1st-Party Fraud

1st-Party Fraud Definition:
1st-party fraud is when the actual account holder or identity owner is also the bad actor committing the fraud.

60% of risk and fraud teams don't have adequate engineering resources to create, test, and update rules to combat evolving fraud in real-time.

This results in reactive countermeasures using rules that create more false positives.

There is a better way.

Unit21 has out-of-the-box real-time rules for common 1st-party fraud scenarios, allowing you to get started immediately:

1st-Party Fraud Scenarios + Rules

Fraud Scenario	Description	What this rule does
Application Fraud	**Fraudster tricking the victims into willingly making large bank transfers to them.** So we want to track outbound transaction right after login that is out of the pattern in terms of amount.	IF Registration days < 7 AND Login Session > 1 AND Outbound transaction count in past 1 hour > 5
		IF Registration days < 7 AND Login Session > 1 AND Outbound transaction count in past 1 hour > $5000

Fraud Scenario	Description	What this rule does
New Account Fraud	User that **just registered recently** that has a high risk score	User that registered within the last week and has a risk score > 88
New Account Fraud	**High transaction volume** within a time window for a new user	User onboarded in the last 48 hours and has transacted more than 7.5K in the last 90 minutes
New Account Fraud	**Few transactions received** for a new account	Fewer than 2 transactions received in the last week for an account registered at least 1 week before that

How Real-Time Rules Can Stop 1st-Party Fraud (con't)

1st-Party Fraud Scenarios + Rules (con't)

Fraud Scenario	Description	What this rule does
Money Mule	User sends funds to themselves - over certain amount	User sends over 1K to themself
Money Mule	High number of ACH recipients in India in a short amount of time	User in the US sends ACH transactions to more than 10 different recipients, all in China, within 3 hours
Money Mule	High volume p2p transactions for low count	More than 5K of transactions sent over at most 25 transactions with each transaction at least $150

Fraud Scenario	Description	What this rule does
Restricted IP	Account is triggering payments from a black listed IP address	Flag a payment is made from a known IP address on Unit21's BlackList
Regulation abuse	Flag transactions in close amounts to their regulatory thresholds	Any transaction within 3% of their regulatory threshold in the US (split up by 3 regions). Thresholds are 10K, 15K, and 20K
Bust out Fraud	Several cards linked to a single user in a short period of time	User links more than 5 cards in 1 hour
High-Risk Geography	IP Address equal to black list countries	Flag a payment that is made from a known IP address on Unit21's country BlackList

To learn more, reach out to sales@unit21.ai

Using Real-Time Rules to Stop 3rd-Party Fraud

3rd-Party Fraud Definition:
3rd-party fraud is fraud committed against organization or merchant by an unrelated or unknown third-party.

Unit21 has out-of-the-box real-time rules for common 3rd-party fraud scenarios, allowing you to get started right away.

3rd-Party Fraud Scenarios + Rules:

Fraud Scenario	Description	What this rule does
ATO	High number of login events within short amount of time	User attempts more than 10 logins in a 1 hour span from non-TOR IP Addresses
ATO	Login attempts from different countries	Login attempts from over 10 countries in a 85 minute span

Fraud Scenario	Description	What this rule does
BIN Attack	Bot running Different BIN variations	Bot running Different BIN variations
Compromised card	Average hourly debit card volume is high	Average of at least 2K in debit card purchases in a 1 hour span for medium risk users (50 - 70)
Elderly Fraud	Client over certain age performs a withdrawal/deposit 0.5 times their fraud threshold	User age (>65 years) with withdrawal/deposit (0.5x Fraud threshold): 24h: 10000, 3d: 20000, 5d: 30000
High Risk Geography	IP Address equal to black list countries	Flag a payment that is made from a known IP address on Unit21's country BlackList
Restricted IP	Account is triggering payments from a black listed IP address	Flag a payment is made from a known IP address on Unit21's BlackList
Testing	Large number of failed transactions within a time window	10 or more FAILED transactions in a 1 hour span
Abuse / excessive use	Entity makes a credit card purchase over a certain amount	Entity makes a credit card purchase over $1,500

To learn more, reach out to sales@unit21.ai