IMPROVE YOUR AUTOMATED SCREENING: CREATE SMARTER RULES

●○○

We've produced a three part Insights Series to help you achieve a more balanced approach to fraud management, and better distinguish between fraudsters and genuine customers. Each part looks at a specific step you can take, providing ideas on how to accept more orders, with less fraud:

STEP 1 OF 3

Improve your automated screening: Use the right tools

STEP 2 OF 3

Improve your automated screening: Create smarter rules

STEP 3 OF 3

Make manual review more efficient and effective

Creating smarter, more efficient fraud detection rules is probably the single most important thing that you can do to reduce both the costs of fraud management and the rate of false positives – without accepting more fraud. We've defined some principles for you to consider applying as you create your fraud rules.

HOW TO CREATE SMARTER RULES

1. USE A HIERARCHICAL SYSTEM OF FRAUD SCORING AND FRAUD RULES

We recommend this approach since even the most comprehensive fraud scoring algorithm can't cater to all of the data points that might be relevant to your business, and in most cases you won't know exactly why an order has the score it does. Fraud scoring algorithms can be highly complex, using potentially hundreds of data points, and are generally opaque to everyone other than the skilled analysts developing them.

It helps to use a service or system that:

- **Gives you some information along with each score,** indicating the key data points that have influenced the score.
- **Has algorithms tailored to different geographical regions, order channels and industries,** since tailored algorithms are generally more accurate.

But however confident you are in the base scoring algorithm that your system or service provides, it is best used as a starting point on which to layer rules tailored to your specific business situation.

STEP 2: IMPROVE YOUR AUTOMATED SCREENING: CREATE SMARTER RULES

2. BUILD TWO TYPES OF FRAUD RULE

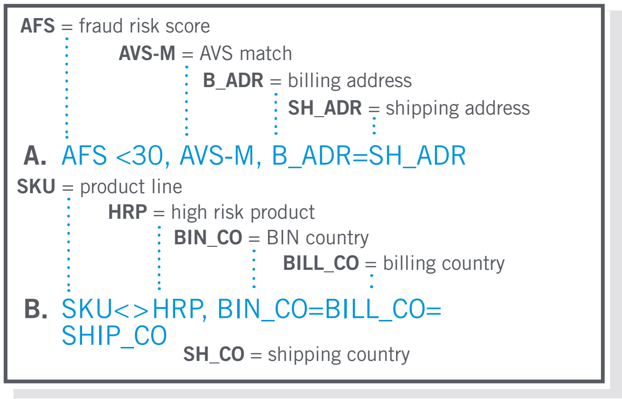
Rules designed to identify genuine orders for automatic acceptance may be transaction-based or customer-based; ideally there should be a mix of both:

Transaction-based rules

These are based on identifying (from first principles and analysis of historical transaction data) the key pieces of data or patterns that, without any other particular context, create confidence in an order. No single data point is likely to be a strong enough indicator on its own, especially with the rise of clean fraud, so it's important to consider multiple dimensions of data that together build a picture of a genuine order.

For example, while an AVS match on its own doesn't mean much, put it together with a match between billing and shipping address, and there's a greater level of confidence. Add consistent device fingerprint geolocation data, or the fact that a loyalty coupon has been used or a low-risk product ordered, and the confidence increases further.

Examples of transaction-based rules that would lead to an order being automatically accepted


AFS = fraud risk score
AVS-M = AVS match
B_ADR = billing address
SH_ADR = shipping address

A. AFS <30, AVS-M, B_ADR=SH_ADR

SKU = product line
HRP = high risk product
BIN_CO = BIN country
BILL_CO = billing country

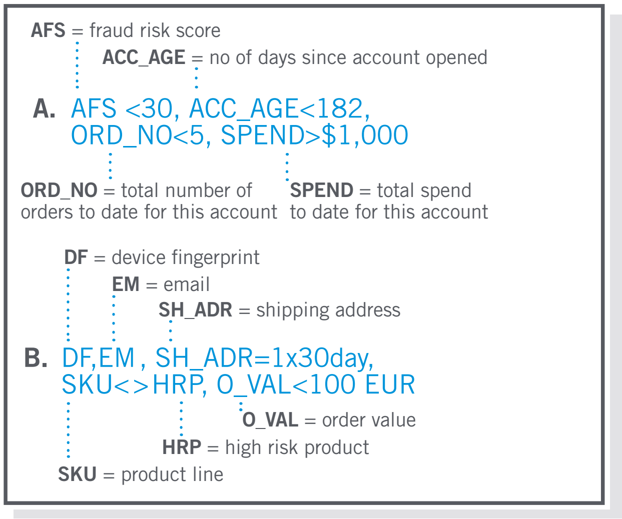
B. SKU<>HRP, BIN_CO=BILL_CO=SHIP_CO

SH_CO = shipping country

Customer-based rules

These are based on analyzing historical transaction data to build up a picture of what a genuine customer, rather than an order, looks like; then turning that insight into rules. Again, it's unlikely that any single feature is sufficient on its own. Look for combinations of data dimensions that indicate a customer profile that should be rewarded with order acceptance.

Examples of customer-based rules that would lead to an order being automatically accepted


AFS = fraud risk score
ACC_AGE = no of days since account opened

A. AFS <30, ACC_AGE<182, ORD_NO<5, SPEND>$1,000

ORD_NO = total number of orders to date for this account
SPEND = total spend to date for this account

DF = device fingerprint
EM = email
SH_ADR = shipping address

B. DF,EM, SH_ADR=1x30day, SKU<>HRP, O_VAL<100 EUR

O_VAL = order value
HRP = high risk product
SKU = product line

STEP 2: IMPROVE YOUR AUTOMATED SCREENING: CREATE SMARTER RULES

○○●

3. DEFINE CHANNEL-SPECIFIC PROFILES

When creating rules, it's important to consider the channel. Some rules will apply across channels. But customer behavior does differ by channel, and failure to address this may result in genuine customers being caught by rules inappropriate to the channel they are using.

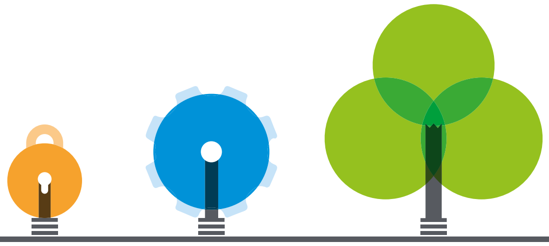
KEY DIFFERENCES BETWEEN mCOMMERCE AND eCOMMERCE CUSTOMERS

Some of the ways in which consumer behavior differs when using mobile devices rather than laptops or PCs are:

- Using the device while on the move, making it difficult to distinguish between genuine and fraudulent orders based on IP geolocation criteria.
- Switching devices in a short period of time, which might be an indication of risk for eCommerce.
- Using the device at different times of the day compared to traditional PC use, which could lead mCommerce orders to trigger time-based rules inappropriately.

4. BUILD IN SAFEGUARDS

Be sure to take a balanced approach. Consider what safeguards should be added to your 'accept' rules, to ensure that they remain potent without increasing your risk. Think of each rule as having a final element – the 'no suspicious activity' element – that calls for appropriate safeguards such as ruling out unusual velocities, recent email changes, or the possibility of a botnet attack.



PROTECT
OPTIMIZE
GROW

To find out more about how we can help you address clean fraud, call us directly or visit **www.cybersource.com/managefraud**

+1 888-330-2300
sales@cybersource.com
cybersource.com