CyberSource®

IMPROVE YOUR AUTOMATED SCREENING: USE THE RIGHT TOOLS

We've created 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

A continuing challenge for fraud management is that fraudsters test systems to discover what data and patterns of behavior are being used to identify them, then find ways to avoid presenting data and behavior regarded as suspicious. The result is 'clean (or sophisticated) fraud'.

THE CHALLENGE OF CLEAN FRAUD

Clean fraud is typically characterized by:

- **Good cardholder data:** it uses stolen payment information with genuine card verification number (CVN) details and sufficient address data to pass standard address verification system (AVS) tests.
- **Valid IPs:** it uses techniques such as botnets to show an IP consistent with the payment data.
- **Strategies to avoid detection:** it avoids the most used behavior markers of fraud, such as short time to departure for travel, retail items of very high value, unlikely purchase velocity patterns, and (often through re-shipping) suspicious shipping destinations.

THE IMPLICATIONS

If data can't be used to distinguish bad from good, the only choice to maintain low fraud levels may be to put in place more stringent screening rules that result either in higher rejection rates for genuine orders, or an increase in manual review of orders (with its higher costs and potential delays in order fulfilment).

THE SOLUTION

Capture and use additional sources of data that let you distinguish good orders from bad through automated screening.

STEP 1: IMPROVE YOUR AUTOMATED SCREENING: USE THE RIGHT TOOLS

HOW TO RESPOND

1. INCREASE YOUR TOOLKIT TO COMBAT CLEAN FRAUD

Use detailed device fingerprinting

First-generation device fingerprinting technologies usually rely on information communicated by a browser to identify a device. Unfortunately it has become straightforward for fraudsters to use proxies to hide the real IP address from the basic fingerprinting process.

- **You can take device fingerprinting to the next level with a packet inspection service.** This can determine whether the transacting device is operating at (or through) a proxy, or has behaviors such as spamming or firewall spamming, associated with machines under the control of another device.

  If these conditions exist, the solution attempts to ascertain additional information about the controlling device – including whether or not it has been previously profiled by the service – and what its true IP geolocation characteristics are.

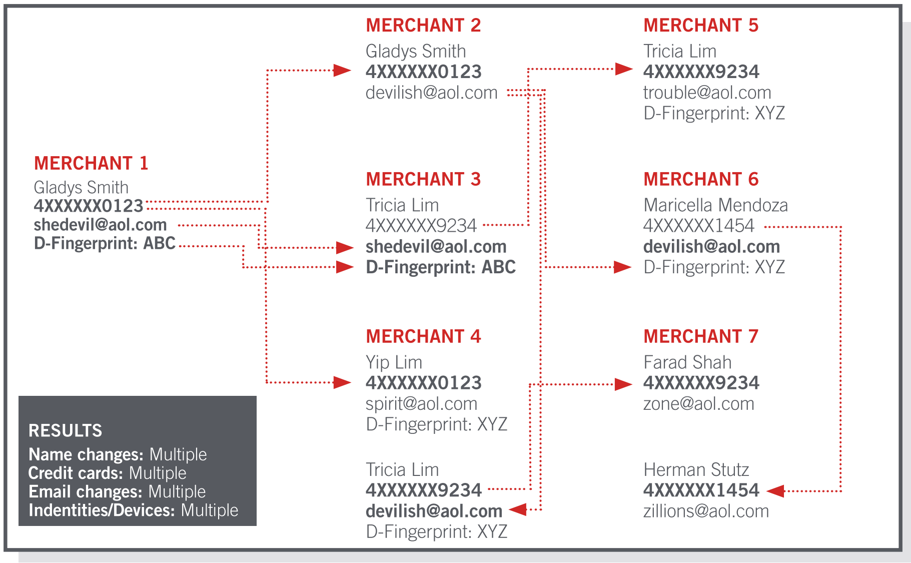
Use cross-merchant data comparisons

Whatever the data being captured – basic payment information, device fingerprints or anything else – the value is multiplied many times over by cross-referencing it with other data sources globally, such as feeds of known infected computers, IP geolocation databases and global transaction histories. This kind of information is indirectly available through some fraud management systems.

This diagram shows how device fingerprint data can be tied to cross-merchant transaction histories to detect fraud. Incoming order information is compared against a broad cross-merchant cache of transaction data (such as names, card details, email addresses and device fingerprints) to identify links and differences in real-time to help recognize suspicious activities.

- **Access to this kind of data can help risk analysts and order reviewers spot likely fraud on a specific order more quickly,** and recognize emerging frauds more easily. It can also be used by fraud scoring algorithms to give a more accurate view of how likely a specific order is to be fraudulent or genuine.

Using cross-merchant transaction comparisons



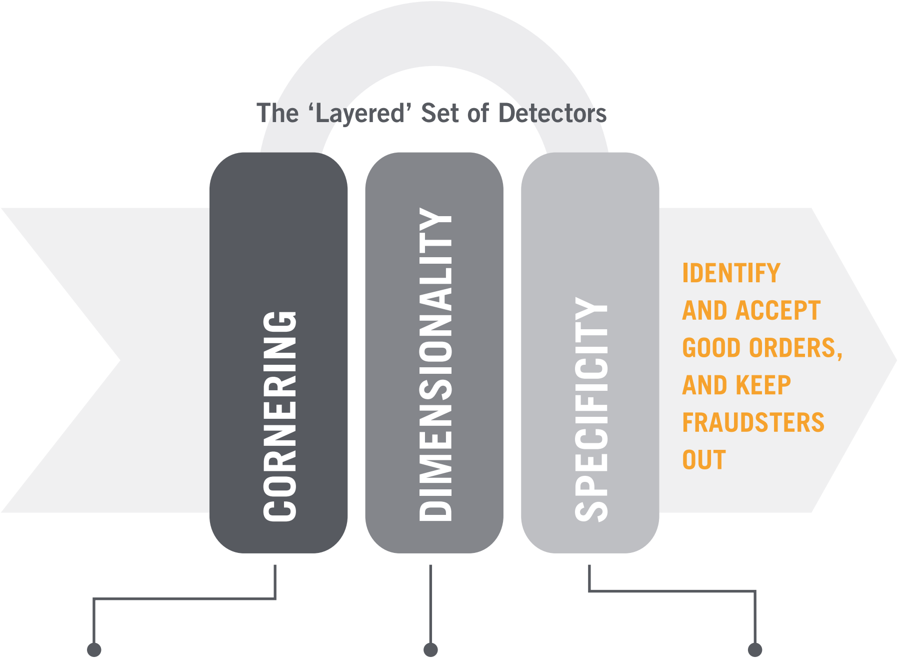
STEP 1: IMPROVE YOUR AUTOMATED SCREENING: USE THE RIGHT TOOLS

○○●

2. USE LAYERS TO DEFEND AGAINST FRAUD

The goal of any fraud management strategy is to accurately identify and accept good orders, while keeping fraudsters out. We suggest a multi-faceted approach or using a 'layered' set of detectors in concert, including the techniques shown here.

A layered approach



The 'Layered' Set of Detectors

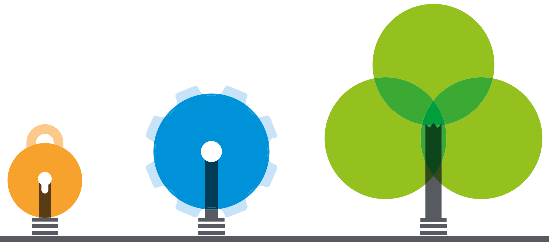
ASK FOR RELIABLE INFORMATION
Force the fraudster to surrender a key piece of reliable information using hard rules (e.g., disable shipping redirect and require that the shipping address is deliverable).

ADD DIMENSIONS OF RELATED DATA
Once you have the key piece of reliable information, add 'dimensions' of other, related data that you have on the order (e.g., device fingerprint, account number, email, etc.), then build rules using these dimensions in combination.

For example, create rules with shipping address + velocity intervals AND shipping address + account number(s).

It makes it more difficult to perpetrate fraud systematically.

CREATE A SAFETY NET
In the absence of reliable or available data, use 'generic' information to create a safety net and assess risk based on the level of information you have. For instance, if shipping address information is not available, create rules around risk levels associated with the postal code or country of the shipping address.



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