GUIDE

IdentityMind™

8 Effective Anti-Fraud Strategies

Introduction

Detecting fraud is not an exact science. It takes years of experience analyzing transactions on a daily basis, dealing with fraudsters and studying their behavior, in order to become an Anti-Fraud expert.

The best source of knowledge for us is the millions of transactions that we evaluate every day from our customer base. This guide describes some of the most effective strategies to detect fraud on transactions, by analyzing the information collected by your ecommerce system when an order is received, and using your Anti-Fraud tools.

Before you start applying the following strategies and tips on your Anti-fraud efforts, we want to emphasize that there are no silver bullets, and not any tip in particular can necessarily be evaluated in isolation, but rather in the context of the overall analysis.

8 Effective Anti-Fraud Strategies

1 Know your customer

Merchants have plenty of information about their customer base that they can leverage for detecting fraud. We know from our own experience that the likelihood of a good customer to perform fraud is very small.

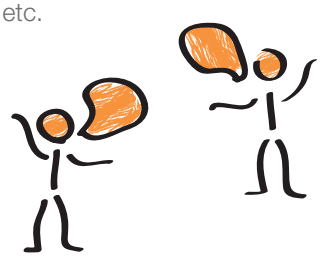
On the opposite side, customers that have performed multiple returns and have been associated occasionally with chargebacks, are more likely to do it again.

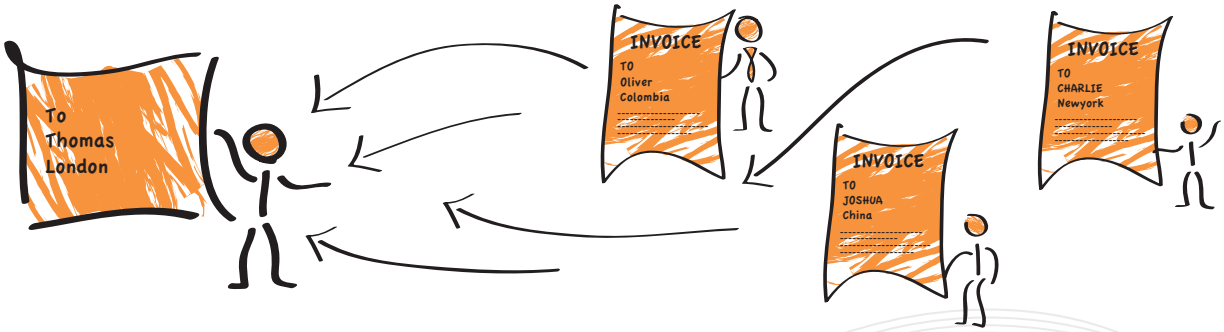
Manual Review Tips

- Contact the customer when in doubt. Good customers usually leave enough information to be contacted.
- Look closely at your order history and quickly move on from good and bad users. Spend your time with users that have little or no history.
- If possible, clearly establish normal operation metrics for your orders, like: time of the day, average order amounts, velocity, etc.

FALSE POSITIVES

Not every order outside the norm is fraud.





2 Same shipping address between different transactions

It is very uncommon to find transactions with shared shipping addresses across users that are not clearly related.

The likelihood of fraud is high when the same shipping address is part of several transactions, and most parameters (e.g. card number, IP address, billing address, etc), are different from transaction to transaction.

FALSE POSITIVES

Corporate Addresses
(e.g. employees send to the same address)

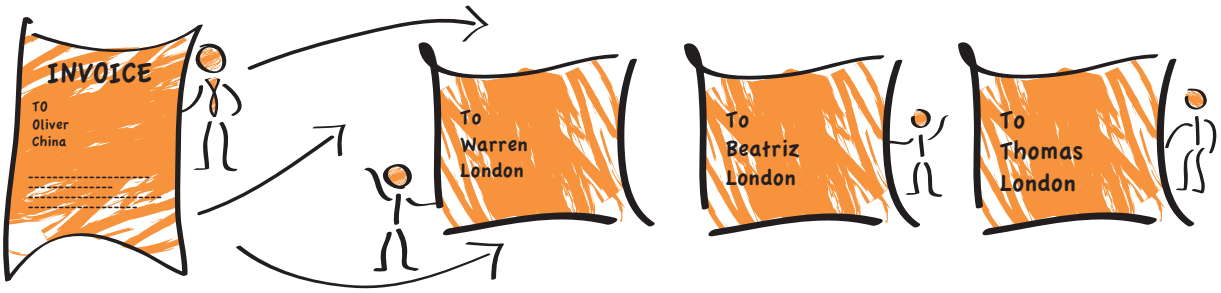
Family Relationships
(e.g. husband & wife with different family names)

Shared Addresses
(e.g. apartment complexes)

Customers shipping goods directly to Freight Forward companies

Manual Review Tips

- To identify corporate addresses you can query the addresses in the Internet using multiple sources. Try to correlate to the email domains where possible.
- Identify family relationships by correlating the billing names and billing addresses of the transactions in question.
- Pay attention to the unit or apartment number if available.
- Validate the address with the postal service or Google™ maps, and make sure it exists and it looks like a real address.



3 Same billing & shipping address but different names

A good indicator for friendly fraud, is when an order has the same billing and shipping address, but different billing and shipping names.

However, it is reasonably common on good transactions too, so you need to watch out for false positives.

An example of friendly fraud is when the kid in the family "borrows" the parent's credit card.

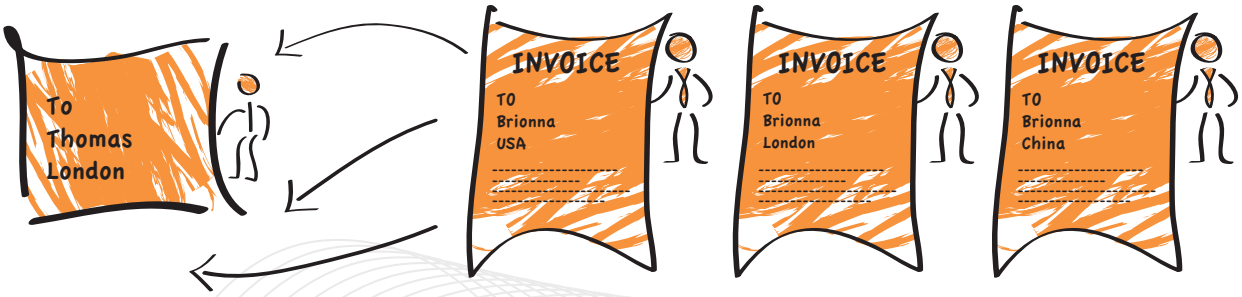
He or she will input the correct billing name and information but it will ship to his/her name.

FALSE POSITIVES

Authorized family members
(e.g. Mom buys gift for son, shipping name is her son's)

Manual review tips

- Check out history associated with the parameters and pull out credit, refund and chargeback historical stats. Evaluate the ship-to names and see if any of them match.
- If you are tracking devices through device fingerprints, see if the device is different from the usual transactions.
- Reach out to the customer using the phone number (if available), validate that is associated with the billing address, chances are that if you can verify the transaction it won't turn into friendly fraud.



4 Same user with different billing addresses

Some users have a couple of billing addresses. However, the large majority of customers, if they have multiple cards, they are all usually attached to the same billing address.

When you encounter a user that has associated multiple cards and each card has a different billing address, you need to take a deeper look at those transactions.

In order to catch these cases, you need attributes that you can use to track a user, like: email address, phone number, device, or the combination of them all. Then you can compare historical billing addresses, and see whether they match or not.

A user with two billing addresses can be considered for manual review…, three or more is most likely a fraudster.

FALSE POSITIVES

The user is using his former address or his company address

Manual review tips

- Check whether the different billing addresses associated with the user are substantially distant from each other. The longer the distance, the higher the risk.
- The billing name might be associated with both addresses in public records.

5 Disposable email address, non-existing domains

Disposable or one-time email addresses are offered for free over the Internet. Anybody can access them.

In general, disposable email services offer a web interface for users to send/retrieve their messages. Unfortunately, there are many of these services, and more pop-up on regular basis, so you need to keep a list of these sites up to date.

In no case should you accept a transaction associated with a disposable email address.

Though email addresses in general don't provide assurance or likelihood of identity, the fact that somebody is really trying not to be tracked through emails, should provide enough doubt to accept a transaction.

An additional check on an email address is the domain itself. Some of these domains are not actually "registered", meaning you wouldn't be able to deliver an email to addresses in such domains.

FALSE POSITIVES

Free service emails

Manual review tips

- You should consider evaluating when the email address comes from a free email service like Yahoo, Google, or Hotmail. The one, and perhaps only, thing you can do is to check the longevity of the email address by using third party databases.
- Certain databases can tell you whether a particular email address has been seen enough in the Internet or not, and from what date they have been seen. The longer it has been around the better chances it belongs to a good user. The less an address has been seen, the more risky it is to trust it.
- Other third party databases can tell you whether the email address has been associated with the billing name, phone number, etc.
- Consider sending an email, if it comes back immediately with a non-deliverable address it might be a non-existing domain.
- Check whether you have had a fraud instance from the given domain (of course, gmail.com may not apply).

6 Phone number analysis

The phone number provided along with the payment information, carries important information that may help you identify fraudulent orders.

It is often considered that consumers are not willing to provide their real phone numbers to the merchants, to avoid further soliciting.

However, statistics show that invalid or temporary phone numbers are much more likely to be associated with fraud.

The legitimate order is more likely to have the real number, as merchants often need to follow up with the customer.

FALSE POSITIVES

Voice over IP phones like Skype or Google voice

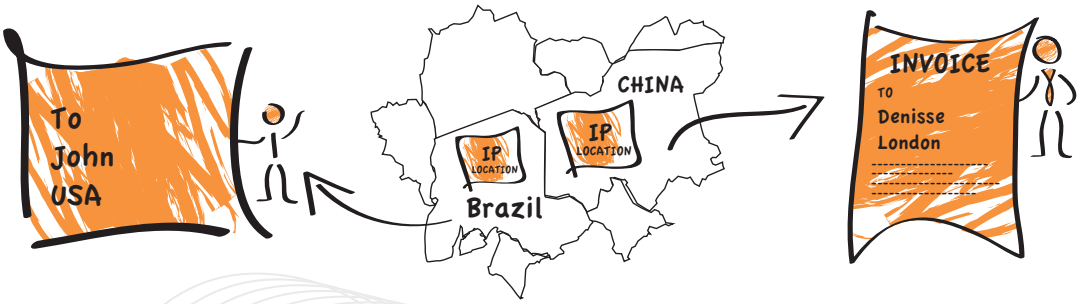
Moving addresses and not changing subscriber address

Keeping phone number through different area codes

IP Geo location associated with Wireless phone numbers

Manual review tips

- Verify phone type: fixed lines and mobiles are traceable and carry low risk. However prepaid, non-fixed VoIP, toll-free numbers, are deemed to be risky and should be either blocked or require additional verification.
- If the phone number is traceable, verify phone country, state, city, and make sure it matches to the billing and IP location.
- Identify the name associated with the phone number, and verify how long the number has been active.
- If the phone number is disposable or invalid, the order should be considered high-risk and shouldn't be accepted.
- If the phone number is international and landline, make sure it reasonably matches the IP Geo location along with the billing/ shipping address.



7 IP location is fairly distant from billing address or country

When the IP address location is relatively far from the billing address location, or the country of IP address doesn't match the billing country, this may be an indicator of fraud.

The challenge here is to be able to measure this distance in the right context.

For example: in Europe, the distance between some countries is less than the distance between two contiguous states in the US.

FALSE POSITIVES

Relativity of addresses

Travelling users. Users roam around for business. These users in particular tend to trigger many fraud filters

Mobile Phones. The IP address given by a wireless carrier doesn't indicate the actual location of the phone. Wireless carriers have "gateways" located in specific geo locations

Manual review tips

- The farther the distance between the IP and the billing address, the higher the chances of fraud.
- Correlate IP Geo Location with shipping address.
- Check the previous history if available, and see if the user is someone who performs transactions from multiple IP addresses. If you find these type of orders, and there haven't been chargebacks associated to the user, then you are probably safe.
- Don't rely on IP addresses when the device is wireless.

8 Anonymous or open proxy

An Internet proxy is usually a software-based service used to hide the original IP address of the user to provide anonymity.

But a proxy may also be a "botted" computer, which is used to hide the original IP location.

Some proxies are services, others are these compromised computers.

There are many valid uses for proxy services, but in general, if a consumer is trying to hide their identity somehow, the likelihood of fraud is very high.

Most of the IP Geo Location services will provide you with an updated list of open/ anonymous proxies.

FALSE POSITIVES

Corporate IP addresses that go through proxies

Manual review tips

- IP addresses associated with anonymous or open proxy are deemed to be of a very high risk. The orders coming from anonymous or open proxies should be blocked.
- Implement device fingerprint and compare the IP address of the order that reach your website, with the IP address of the consumer's computer. Some providers of device fingerprint call this technique proxy piercing.

CONCLUSION

We are confident that you will experience significant improvements on your chargeback rate and the losses associated with fraud, by applying the previous strategies on your transaction's Anti-Fraud evaluation.

However, it will require an important effort from your staff performing Manual Reviews, with the associated cost on your business operation.

The most cost effective protection against fraud will always be a complete and automated Anti-Fraud solution.

Please send us your feedback about this guide, and let us know if you want to be included in our mailing list, to receive communications when we release new content.

Learn more about IdentityMind, and how our PCI Compliant Anti-Fraud Platform detects automatically more than 400 fraud indicators (including those described in this document), combined with our unique Patent-Pending eDNA technology to identify Internet users based on their payment reputation.

IdentityMind, Inc.
1731 Embarcadero Rd, Suite 200, Palo Alto, CA 94303
Tel: 650-618-9977, Fax: 650-618-9976
Sales: sales@identitymind.com

Learn more