

# Fraud Detection in Accounts Receivable Factoring

## Introduction

This document is an overview of how *Detect* can be used to protect organisations involved in the Factoring of Accounts Receivable.

There are two main models for factoring:

- open factoring
- hidden factoring

### Open Factoring

In Open Factoring the merchant does not mind if its customers know if they are using a factor. The factor can then send invoices directly to the debtor to recover the face value of the invoices received from the merchant. The diagram below illustrates the basic scheme.



### Hidden Factoring

If a merchant has decided to factor its invoices in order to improve cash flow, it may be concerned that this is not apparent to its customers. In this case the debtor is invoiced by the merchant, not the factor. The factor is sent the invoice in the normal way and then pays the agreed percentage. When the debtor finally settles their invoice the sum due to the factor is then paid. In practice, the sum due may be simply deducted from the next payment due to the merchant by the factor.



### Export Factoring

In the above the Debtor may be in a separate country to the Factor and Merchant. In these circumstances other types of fraud in addition to those described below can take place, such as over and under invoicing.

## Fraud Types

The factor is taking on several kinds of risk when paying the merchant, including the risk of fraud. Both models of factoring are vulnerable to many types of fraud.

### Collusion

Many types of fraud are only possible if there is collusion between several parties. Collusion can take place at many levels. The following example of fraud requires the collusion of the merchant and the debtor. This is probably the most common type of collusion.

In order to make a fraud less detectable the merchant may use many different debtors. The pre-requisite collusion for the fraud then appears to be absent. Although the debtors may appear to be different they may either be in collusion or are all owned or run by a common individual or company that is in collusion. This would be an example of second-level collusion. Much more complex relationships can be used to obfuscate the fraud.

The problem of collusion is very similar to that posed by Money Laundering. Both require the detection and evaluation of relationship-networks.

### Lapping Fraud

Lapping is the name given to fraud schemes where an initial fraud is then covered up by a subsequent fraud, which in turn is covered up. The sequence continues and usually the amounts will grow very quickly.

For example:

If we assume that this is a Hidden Factoring agreement whereby the factor pays 90% of the face value of the invoice within 2 days and that the due-date of the invoice for payment by the debtor is 30 days.

1. The merchant raises a fictitious invoice against a company (aka debtor) for 100,000.
2. The merchant sends the invoice to the factor for payment.
3. The factor pays the merchant 90,000
4. The merchant needs to pay the factor 100,000 in 30 days. The merchant therefore raises a further fictitious invoice after 25 days (not necessarily against the same company) for 130,000
5. The factor pays the merchant 117,000
6. The merchant can then repay the first invoice value of 100,000 and still has 17,000

The process repeats itself with each fraud covering up the previous fraud and with the invoice value continually growing. In fact the invoice value must grow by the percentage due to the factor as a minimum for each invoicing iteration. The irony is that it could look like the merchant's business is doing well to the factor, who may then reduce the percentage on each invoice and thus making the fraud easier for the merchant.

In the above example it was assumed that the factoring agreement was hidden, hence the factor has no direct relationship with the debtors. Lapping is also possible with an open agreement but the debtor company has to be either in collusion with the merchant or the debtor company may well be a shell company set up by the merchant to perpetrate the fraud.

## Other Frauds

There are of course a myriad fraud schemes limited only by the imagination of the perpetrators.

## Detecting Fraud

The following is a brief overview of some of the methods *Detect* can employ to detect various types of fraud that are specific to factoring. Other, more general, detection can also be employed as outlined in the paper on invoicing fraud.

*Detect* uses both rules and statistical machine-learning to determine the risk of fraud. The Risk Engine can learn from historical data, while the rules, known as Patterns within *Detect*, will alert the occurrence of known static indicators in the transaction stream.

*Detect* needs to look for trends and patterns in the Merchant Account data (within *Detect* this would be regarded as a channel) and within a Merchant's Debtor data (within *Detect* this is a stream) and also the complete history of a debtor. These are the main time-series that the system uses but others can be added as appropriate.

## Collusion Detection

The following describes some of the methods for detecting collusion. It should be borne in mind that it is very easy to add new patterns in the light of an analyst's domain-expertise and knowledge of the particular client-base.

1. postcode of merchant are the same or are geographically close to those of a debtor
2. postcodes of different debtors of a merchant are the same or are geographically close
3. telephone of merchant are the same as those of a debtor
4. telephone of different debtors of a merchant are the same
5. several new debtors for a merchant
6. violations of Benson's Law as applied to invoices values

## General Fraud Detection

Example measures

1. large invoice value relative to mean for that debtor
2. large total invoice value relative to mean total value for that debtor
3. new debtor with rapidly increasing invoice value
4. profiling of count-rate of invoicing, by merchant category for merchant
5. profiling of value-rate of invoicing, by merchant category for merchant
6. profiling of count-rate of invoicing, by merchant category for debtor
7. profiling of value-rate of invoicing, by merchant category for debtor

## Lapping Fraud Detection

Fraud of this type must grow at a minimum rate as defined by the percentage due to the factor.

1. Any consistently increasing invoice value to a particular debtor.



2. Where several debtors may be involved, then we aggregate the invoices across the collusive set of debtors

## Data Integrity

The performance of any system relies on the quality of the data. *Detect* can be used to pre-process data to look for inconsistencies. Patterns (aka rules) can be used to set up to trawl through historic data and alerting anomalies. *Detect* also includes various other statistical methods for mining a data set that can be used to check historic data.

## Appendix - General Invoicing Fraud

Invoicing fraud can take many forms and can be perpetrated by individuals both within and external to the organisation affected. Some examples are:

### Internal Fraud

A simple example is an employee who has the authority to raise purchase orders will raise purchase orders for some fictitious company that they will have previously set up. The company then raises invoices against these purchase orders that will then get matched and honoured.

Internal fraud often leaves a trail:

- Various documentation will carry a forged signature.
- Unrecognised signatures
- Cheques drawn out of sequence
- Access to computer or premises at unusual times
- Returned cheques with alterations
- Use of staff bank accounts and/or addresses

### Counter Measures

purchase profiling	by profiling purchase patterns we can detect, for example, unusual quantities of a particular type of supply being ordered.
supplier profiling	by profiling supplier invoicing patterns we can detect changes that may be indicative of fraud.
whitelists	whitelists are used to reduce the incidence of false positives for trusted suppliers.
staff details	use staff lists, payroll details to find patterns relating to invoicing details

### External Fraud

An example of an external fraud is an employee working for a supplier of an organisation who registers a company with a very similar name to the company they are working for. They then issue invoices against known purchase order numbers with this name.

### Counter Measures

automated checking	precise matching and cross-checking
... also as per	internal fraud

### Double or Duplicate Invoicing

A supplier sends in an invoice, then sends it again with a subtle change so that it may not be noticed that it is from the same supplier.

Large organisations that employ many itinerant workers, directly or through agents, will receive invoices for hours worked. Authorisation of an invoice is often not supported by a

purchase order and there are many ways to exploit this. For instance some cultures, eg Hungary, put their surname first and their given name last. So one common form of duplicate invoicing in these circumstances is to raise two invoices, one for each name order.

Another example is multiple invoices against the same purchase order.

**Counter Measures**

matching	fuzzy name matching, rule-based matching
supplier profiling	supplier category profiling
... also as per	internal fraud

**Purchase Order Value**

The Invoice value is much greater than the purchase order value. It may simply be ten times the purchase order value, which can easily go unnoticed.

**Counter Measures**

automation	automated cross-checking
------------	--------------------------

**Unknown Vendors**

Organisations often receive invoices from unknown vendors for fictitious work or goods. The senders of the invoices may have sent the same invoice to hundreds of organisations in the hope that just one busy accounts department lets it slip through.

**Counter Measures**

... as per	internal fraud
scheme matching	known fraud scheme matching

**Unsolicited Goods**

Goods are delivered and signed for and then an invoice is sent. The sender will often have some knowledge of the organisation's regular supply of consumables or current projects.

**Counter Measures**

... as per	internal fraud
scheme matching	known fraud scheme matching

**Low Value Invoices**

Many organisations try and manage the workload associated with invoices by operating much stricter authorisation procedures for invoice values above a threshold. Invoices that are

received whose value is below this threshold are much more likely to get authorised and a potential fraudster will exploit this information, which may be gleaned from an employee or by sending test invoices or a disgruntled employee who may have already left the company.

**Counter Measures**

purchasing patterns	inappropriate frequency of invoicing for category of supplier.
... as per	internal fraud

**Under or Over Invoicing**

This is not really a type of invoicing fraud, more a type of tax fraud. Under-invoicing is used when importing goods from a foreign supplier. An arrangement is made whereby the supplier raises an invoice for the goods with a value much less than the agreed price. By artificially lowering the documented value of the goods less import duty is payable. The difference is then paid via a different route and sometimes the saving in import duty is split between the importer and the supplier.

Over-invoicing is a means of exploiting exchange rates and export subsidies.

**Counter Measures**

purchase profiling	by profiling purchase patterns we can detect, for example, unusual quantities of a particular type of supply being ordered.
supplier profiling	by profiling supplier invoicing patterns we can detect changes that may be indicative of fraud.
whitelists	whitelists are used to reduce the incidence of false positives for trusted suppliers.
staff details	use staff lists, payroll details to find patterns relating to invoicing details