aronova.com

Fraud Monitoring

Using modern technology to harness the power of data brings many benefits, yet it also comes with risks. Fraudsters know this and do everything they can to exploit these weaknesses.

Receivables-backed finance is a good example. Deception is more common than we'd like to think and is often hidden in the detail of large data volumes and the complexity of how these receivables programs actually work.

As fraud is not typically covered by trade credit insurance, counter-parties to these transactions are highly exposed to fraudulent sellers. Sadly, it's the funders who ultimately bear most of the burden of this ever-present risk.

So, what can organizations do to protect their investors and their investments? Data holds the answer. When fraud lurks in the detail, understanding and systematically tracking that data helps to uncover issues. By identifying the signs of potentially fraudulent behavior, appropriate action can be taken to avoid falling victim to questionable seller actions.

ARONOVA

INNOVATION IN WORKING CAPITAL FINANCE

WHITE COLLAR FRAUD

Most receivables finance frauds are based around fresh air invoicing or seller-debtor collusion. But other types of fraud are increasingly pervasive, mainly because traditional risk management tools are completely blind to them.

Funding programs often control risk by setting eligibility criteria; rules that determine which invoices can be funded, and these newer frauds involves the subtle manipulation of individual data points to falsely pass eligibility testing.

For example, a program funds invoices with a maximum 90-day tenor. The seller presents a 75-day invoice, which passes eligibility and is sold. Post funding, the seller changes the due date, correctly setting the invoice tenor to 120 days.

So is this honest data input correction or more sinister manipulation of data to make otherwise ineligible invoices eligible?

VICTIMLESS FRAUD

Sellers often don't consider this as fraud; they're harmless data tweaks, there's no victim and nobody's the wiser … right? Wrong; the funder is now exposed to a layer of unexpected risk that's invisible to traditional program management.

The only way to effectively mitigate this type of risk is to implement a more rigorous approach to data monitoring, and by using technology to automate how funding programs respond when data anomalies like these are detected.

A simple daily report that highlights key anomalies can often prompt a discussion with the seller. And its funny how, once the seller knows we monitor for these anomalies, they suddenly stop occurring!

The temptation to commit white collar fraud can sometimes be overwhelming to a seller in need of more funding.

KEY FEATURES

Anomaly Detection

We track every change to every invoice, irrespective of invoice status or when the change is made. Each program has its own rules for determining 'anomalies'.

Mandatory Repurchasing

When anomalies are detected, each program can set rules to determine how anomalies are treated, including the option to auto repurchase.

Anomaly Reporting

Daily reporting can be generated that summarizes identified anomaly incidences per seller. Program settings can determine anomaly sensitivity.

Anomaly Definition

Each program has its own definition of anomalies. Some anomalies definitions are binary – has this or that occurred, while others test for degrees of change.

If you would like to know more about Aronova or the services we provide, please visit www.aronova.com, or contact David Baker, Managing Director, on **+44 7739 173 961** or **+1 848 466 5288**, or email David at **david.baker@aronova.com**