Fraud in Accounts Receivables: Prevent, Detect and Eliminate Risk and Avoid Damage

By: Garoid Pierse
Senior Solution Architect
Serrala

As originally published in the Credit Research Foundation Q4 2019 CRF News

Digital technology is vastly transforming and disrupting economies all around the globe, exposing organizations to both opportunities and threats. It comes as no surprise that, just like every other aspect of business, economic crime is going digital. Modern-day hyper-connectivity offers entry points for cybercriminals and fraudsters, enabling them to compromise an organization's digital landscape in various ways. Possible breaches can appear anywhere in the digitally transforming economy. An example would be attacks on devices enabled by the Internet of Things (IoT), including cars and household devices. Breaches can also occur with mobile and eCommerce services, cloud computing or even with traditional on-premise ERP systems.

Fraud and Cybercrime on the Rise

This persistent and pervasive threat leads to what has been called the *digital paradox*. Organizations are in a position to benefit from new digital connections, tools, and platforms which can connect them in real time with customers, suppliers and partners. Yet, at the same time, cybercrime has become a powerful countervailing force that threatens this potential. Awareness of this paradox is growing: Six in ten chief executives rank both cyber threats and the speed of technological change as top threats and challenges to their growth, according to the 19th Annual CEO Survey by PricewaterhouseCoopers (PwC). Approximately one-third of organizations have been the victim of fraud in the past few years, illustrating that economic crime is changing significantly and that detection and control programs are not keeping up with the pace of change.

Additionally, the financial cost of each fraud case is on the rise. A major problem is that companies are not handling fraud and economic crime with the priority it deserves. In fact, 22% of companies surveyed have never carried out a fraud risk assessment and a further 31% of companies only carry out such an assessment annually, according to PwC. It appears, therefore, when it comes to fraud, too much is being left to chance. After all, the same report indicates that one in ten economic crimes are merely discovered by accident.

While asset misappropriation, cybercrime, bribery, and corruption make up most of the reported economic crime, procurement fraud and accounting fraud follows closely with 23% and 18% respectively. It is of paramount importance therefore to secure inbound payments to effectively protect the organization's overall payments ecosystem from fraud and economic crime. As the legislative landscape continues to change, businesses will face additional regulatory challenges and must be prepared to protect themselves and their business relations from the dangers of economic crime.

Fraud in Accounts Receivables: What to Look Out For

Although fraud attempts are often directed at outbound payments by external actors, fraud in inbound payments, which is conducted by employees, should not be disregarded. According to the PwC Global Economic Survey 2016, fraud and theft are more likely to be committed by an internal actor than an external actor, with senior and middle management representing the largest source of internal fraud.

Consequently, every organization needs to ask itself to which degree its existing order-to-cash (O2C) processes are prone to fraud risk, because neglecting those risks can be detrimental. The constant influx of cash in accounts receivables (AR) makes this area very vulnerable to internal fraud risk. Without the right checks and balances in place, intentional theft or misappropriation of company revenues can become a serious threat. In fact, AR fraud schemes are among the most common forms of employee theft, yet most companies do not have standards in place to prevent them. Undetected AR fraud can result in a significant disruption of your cash flow and even threaten the very existence of the company. Typical AR fraud issues to look out for include:

- **Insufficient separation of duties:** Employees who are responsible for both collecting and posting payments can easily steal incoming cash and manipulate the bank reconciliation process to make up for the missing amounts.
- **Diversion of payments:** Redirecting incoming cash to old or slow paying accounts that companies typically do not keep track of can also be a lucrative fraud scheme.
- **Refund skimming:** A common scheme is to pocket refunds that are meant for companies that have accidentally overpaid.
- **Check skimming:** Intercepting an incoming check from an account holder and cashing it to a private bank account is classic fraud attempt.
- **Lapping:** Employees have been known to divert customer payments to cover up a theft or misuse of a previous customer payment.
- **Fraudulent write-offs:** Employees might conduct false write-offs to cover up a previous theft.
- **Fictitious sales:** This technique might be applied to receive commission-based compensations or to make a company appear to be in better financial shape for creditors and investors.

As shown, AR can provide several entry points for fraudsters to steal incoming money, endangering the company and distorting its overall liquidity. It is therefore important for companies to look at fraud and economic crime for both outbound and inbound payments.

How to Stay Safe: Best Practices in Fraud Management

Protecting your O2C processes from fraud cannot be managed by accounts receivable managers alone. Different stakeholders and responsibilities come into play, such as global finance process owners, compliance officers and, of course, IT. The following overview represents some best practices that will help your organization to protect their accounts receivables.

Systematic Risk Detection

Anomalous transactions keep changing patterns frequently. To prevent fraud, companies have to stay on top of such changes at all times so they can detect anomalies quickly and block them. Ideally, an automated detection process could be put in place to recognize suspicious behavior, for example, when money is moved to accounts that have been inactive for a long time. To enable automated detection, transaction data should to be centralized and continuously analyzed to identify any unusual loss. Automated alerts also then can be set up to inform multiple account managers when potential fraud is detected, so that the findings cannot be hidden by the fraudster.

Standardized Processes and Compliant Execution

Processes also have to be monitored to make sure that standards and codes of conducts are not violated. Since the risk landscape is so multifaceted, it is not enough to ensure that the customer onboarding or collections processes are safe. To be truly on top of things, organizations have to eliminate weaknesses in the entire O2C cycle – without harmonized end-to-end processes, companies are at risk of losing money.

Centralized Inbound Payments

To keep incoming cash extra safe, companies are well advised to implement best practices for cash forecasting. These processes will ensure companies do not have excess cash in their global bank accounts. Damages resulting from fraud can be mitigated significantly by concentrating the majority of cash into centralized accounts and topping up operative accounts as needed.

Definition of Responsibilities

Best-in-class companies assign process owners who are responsible for both the performance and the integrity of the processes. Equipped with a strong mandate from the management and with clear responsibilities, these process owners should have the authority to not only enforce the business process but also the policies for governance, risk management, and compliance (GRC). In the case of data breaches, it will be easier to organize reactive measures with a single process owner. Organizations should also define and put in place strict approval processes, specific policies and the necessary user roles and access rights.

Auditability and Process Documentation

Documenting your current processes carefully is time well spent. It can reveal inefficiencies, security issues, and irrelevant steps but also non-compliant behavior and fraud attempts. Furthermore, it helps companies to standardize their processes and align them with industry best practices. Improving processes and making them auditable ensures any error can be traced back to the responsible party.

Conclusion

Securing inbound payments requires a holistic view of the processes, technology, people, policies and corporate values involved. Risk in O2C processes cannot be mitigated if the processes remain siloed. Security must be a guiding principle across all O2C operations. While automated processes and end-to-end solutions play their part in securing inbound payments, centrally managed user rights and rules are just as important. Organizations must be aware of the potential risks and be prepared to invest both money and time into fraud prevention at each step of the process. Today more than ever it is the only way to ensure that accounts receivables are secure and effectively protected from fraud attempts and economic crime.

About the Author:

Garoid Pierse, *Senior Solution Architect, Serrala has 21 years SAP Finance experience, specializing in Banking, Treasury and Tax. He has worked on global SAP projects with PwC, IBM and Tech Mahindra. In addition to numerous SEPA implementations in EMEA, Garoid has implemented Payments from SAP systems in 14 APAC countries. In September 2016, Garoid joined Serrala as a Senior Solution Architect, advising current & potential clients on how best to transform, automate and simplify their payments processes.*