glantus
Liberate. Innovate.

WHITE PAPER

LEVELLING UP ON FINANCIAL FRAUD AND COMPLIANCE

Fraud Prevention by Design

It will come as no surprise to learn that financial fraud is on the rise. As we conduct more business outside of the office and operate as virtual teams, this can give rise to higher IT and data security risks that increase exposure to new (and old) types of fraud. All of these elements, combined with legacy compliance processes designed to combat financial crime - create complexity that is difficult for finance teams to manage.

According to the latest research, 38% of businesses reported a business payment fraud attack over the past year. That's close to half of all organisations surveyed, in fact the figure is likely to be a lot higher in reality, as many companies do not like to share their experiences with fraud. However, it is worth understanding that not all of these payment fraud attacks succeed and raising awareness of the risks that exist, helps to make sure that your business is protected.

Improving Accounts Payable (AP) reporting and data analytics was reported by 55% of organisations as their top priority for AP in 2022. From a fraud perspective, this helps to significantly reduce the most prevalent risks, as invoice and B2B payment fraud remain the most likely type of financial fraud within AP today. According to Bain & Company, having a strong financial crimes compliance strategy that includes some form of partnership with a specialist technology provider is key to minimise the risk of financial fraud and breaches of regulatory compliance – that can lead to fraud, fines, or both!

Having intelligent systems in place to raise a red flag as early as possible when an invoice arrives is the best way to combat the problem and technology has proven to be a valuable way to prevent, or at least minimise this type of fraud. The latest Machine Learning (ML) algorithms are designed to identify even the slightest difference between a typical invoice from a supplier and the one that has just arrived, to sniff out potential fraud before it gets through the gate. Then there are ongoing validity checks, along each stage of the invoice processing, approval, and payment cycle that minimise exposure to risk.

Another type of fraud that is on the increase is social engineering attacks. Phishing attempts and business email compromise (BEC) have increased by 33% since 2020, according to Forbes. The targets can vary from consumers and retailers to employees and even company executives - through what is known as "CEO fraud". CEO Fraud is a request, often made via email, purporting to come from a senior person in the company, normally to the accounts department, requesting an urgent payment to a supplier or partner. Depending on the company, processes, and levels of awareness to fraud, this type of financial fraud is a significant risk to the business and was responsible for $2.4 billion in losses to U.S. businesses alone, in 2021.

The sophistication of financial fraud has increased but so has the technology that can help prevent these attacks from succeeding. The purpose of this paper is to help you to understand the risks of financial fraud that exist in business today, and also learn how to manage them effectively, through a combination of people, process, and technology.

The Background

In the second half of 2020, the average number of BEC attacks received per company, each week, rose sharply by 15%, compared to the previous 6 months. More worryingly, attacks that employed invoice or payment fraud increased by 155%, to become the most pervasive type of BEC risk.

Business email compromise can arrive in many forms and can tie directly into invoice fraud scenarios. Email fraud has been around for a long time, but BEC makes it much harder to detect. For all intents and purposes, an email coming from your trusted suppliers' email address, with wording that mimics their tone may not be seen as suspicious to the naked eye. However, the metadata associated to the email, the document properties and underlying information can allow a technology-based system to weed out these entry points to potential fraud and avoid any losses for your company.

The 2021 Payment Threats and Fraud Trends Report from the European Payments Council highlights the risks relating to invoice fraud, stating that "invoicing and Request-to-Pay (RTP) are particularly exposed to fraud as they rely on the trust between the Payee and Payer and the security of the environment in which this information is exchanged".

Therefore, the first point of contact is the most critical time to protect your business. The SPAM filters that were effective for unknown or untrusted email domains cannot identify fraudulent emails coming from trusted email addresses and entering your AP process. This is where you need to get specific about the technology that can deal with the problem in a way that won't create high levels of false positives, a frustrating issue that exists in many of the software solutions out there.

Fraud Prevention by Design

The main causes of financial fraud normally come back to the same things; lack of validation, time pressure, supplier demands, and lack of awareness. These are the things that contribute to losses incurred through fraud in AP. As the level of sophistication increases in how financial fraud is executed, people need to be supported in their role to protect the revenue within their business.

Here are some of the most effective measures to combat fraud:

- Reconcile and audit accounts regularly, for early detection of compliance issues or potential fraud.
- Scrutinise all incoming invoices, ideally using intelligent automation.
- Avoid soft overrides that bypass systematic checks.
- Automate the confirmation of payments to vendors, with the amount and account credited.
- Establish two points of contact with each vendor, confirm any major changes directly.
- Deploy a system to monitor all vendor master information updates, especially bank details.

Companies that follow these measures will reduce their level of exposure to fraud by approximately 25%, compared to companies that do not incorporate these steps.

Fraud Prevention Awareness

These days, a lot of companies promote security and data protection awareness, training, and education wherever possible. This should include warnings for phishing attacks, and encouragement to adopt security measures (such as MFA) on all devices. Fraud awareness campaigns should be built into a cultural approach for the organisation and not just a once-off presentation or annual session, the approach to financial fraud evolves every day and people need to be reminded of this.

Conclusion

Current best practice for financial fraud prevention includes regular process and compliance audits, along with automation of statement reconciliation, detection of duplicate payments, and monitoring vendor master files to guard against invoices from inactive suppliers. However, the people behind fraudulent activity will keep coming up with new ways to successfully commit fraud and cost companies' money, time, and trust – inside and outside of their organisation.

Financial fraud cannot be fully de-risked, but by taking these steps to mitigate the most likely entry points – you are taking proactive measures that will protect your business.

Written By

JOE KEATING

Head of Customer Experience,
Glantus

Find out more at
Glantus.com

UK: +44 203 7874457
IRL: +353 1 889 5300
US: +1 646 893 5970