# Preventing fraud
## a board's duty of care

Sam MacGeorge
CEO of Vigilance Ltd

VigilantPay

www.VigilantPay.com

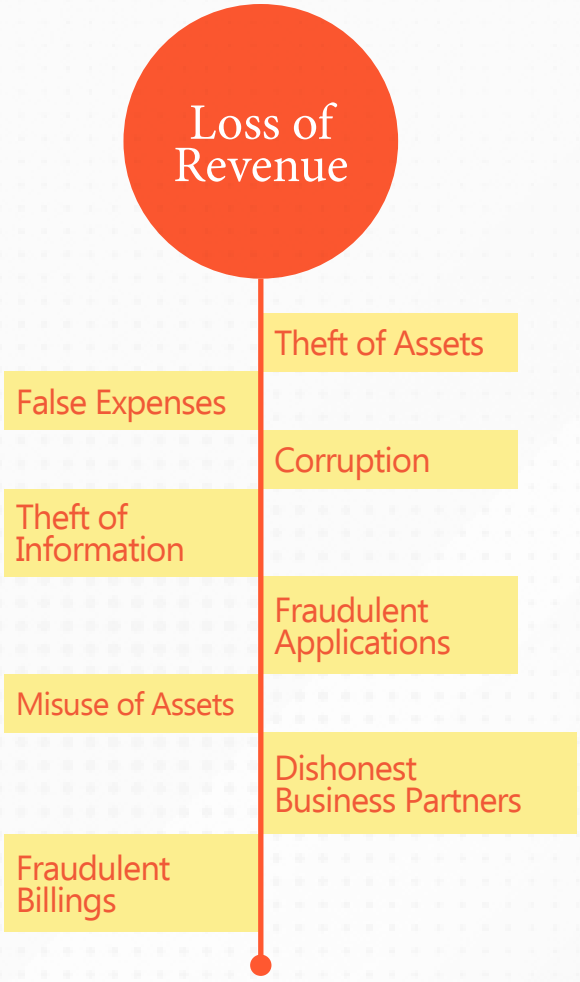
This whitepaper explores the impact and cost of payment fraud, the difference between internal and external fraud and why good organisations get caught out.

# Do we have protection methods in place?

Ask your board if they know what fraud prevention methods the organisation has in place to protect their cash and the answer is likely to be vague.

Ask senior management if they understand the organisation's payment processes and you are more often than not going to find they don't really understand the mechanics.

Ask an employee in Payroll or Accounts payable if they understand how payments are processed and they will give you a step by step account of the process. If pressed they would also be able to tell you the shortcuts, weaknesses and work-a-rounds in the systems and procedures, and how they could easily take advantage of these should they wish.



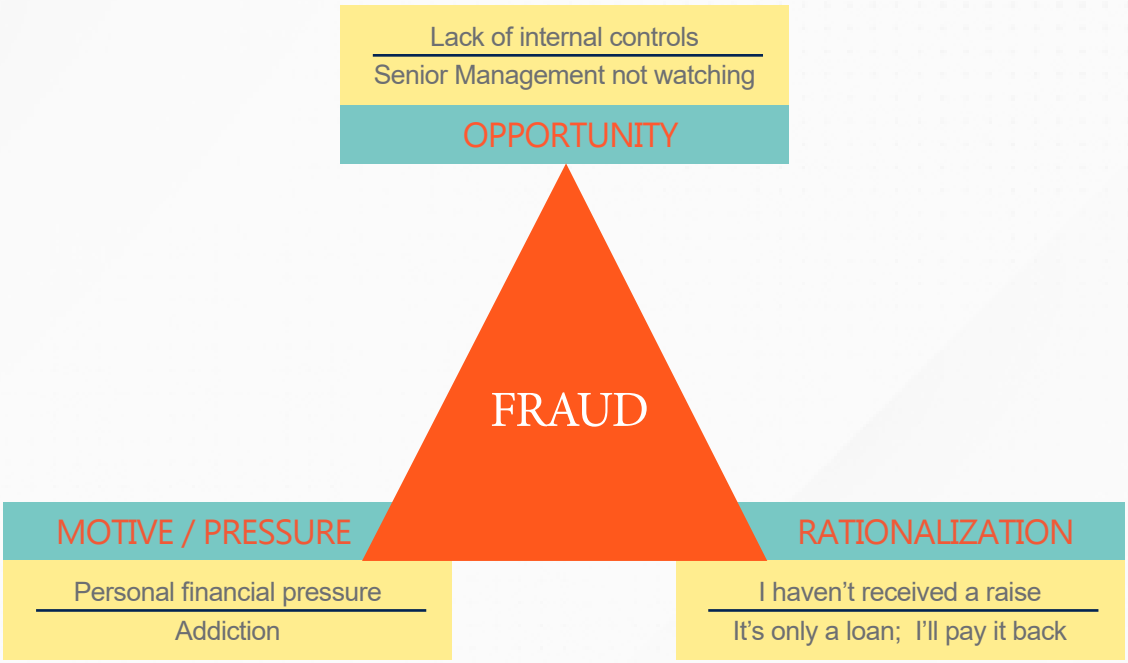

## Unquestionable Trust

This expectation gap exists because of the unquestionable trust management has with the people and processes throughout an organisation. Staff come and go and with this other processes often get introduced, documented processes are not followed (or never existed) all because we are only human, and we get busy.

The opportunity for payment fraud already exists, one only needs motivation to become a fraudster. An otherwise good employee's dishonesty is often triggered by a change in their personal life where they need money quickly and have exhausted access to the normal channels. Whereas external fraudsters are driven by greed, and work on a hit and miss approach. The big difference is the former will persist and often these frauds will go undetected for many years.

# The Fraud Triangle

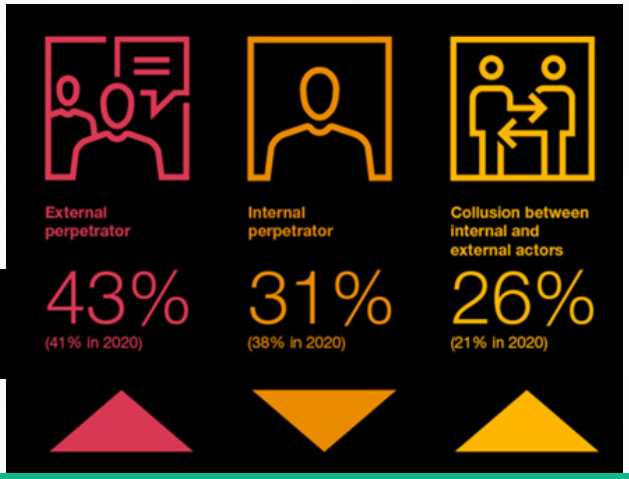
Interestingly many internal frauds are committed by an employee who has no criminal record however it's motivation followed by rationalisation which becomes the self-justification for continuing to take company money once the fraud has started. This is the classic modus operandi of internal fraudsters commonly referred to as the fraud triangle by forensic accountants and auditors.




The COVID era has key staff often working from home or management not always in the office to keep an eye on things. This further reduces transparency and introduces changes to processes, unlikely to have been tested from a risk perspective. Now we are facing a period of high inflation adding more financial pressure to households and with it an increased motivation to potentially steal company money

Payment fraud is either perpetrated from within or from an external actor, the latter typically by email compromise such as invoice fraud or impersonating a manager requesting an urgent payment through an email. The risk of payment fraud is at an all time high and businesses are exposed to one or both from taking place, if not already.

A recent PwC's Fraud Survey[1] , stated that internal invoice fraud is now almost as common as external invoice fraud with 43% external perpetrators and 31% internal perpetrators.




1. https://www.pwc.com/gx/en/services/forensics/economic-crime-survey.html

# External Threats are on the Rise (PwC Online Article)[2]

"Preventing fraud and other economic crimes is a complex challenge, complicated even further by today's volatile risk landscape. As organisations act quickly to navigate change, bad actors look to exploit the potentially widening cracks in fraud defenses."

**46% of surveyed organizations reported experiencing fraud, corruption or other economic crimes in the last 24 months.**

"PwC's Global Economic Crime and Fraud Survey 2022 shows good news: the proportion of organisations experiencing fraud has remained relatively steady since 2018. However, the survey of 1,296 executives across 53 countries and regions found a rising threat from external perpetrators—bad actors that are quickly growing in strength and effectiveness. Nearly 70% of organisations experiencing fraud reported that the most disruptive incident came via an external attack or collusion between external and internal sources."

# Complex Backoffice systems

Businesses generally do have good systems and processes in place however they are only as good as their limitations. ERP, Payroll and Banking platforms are siloed from each other and don't talk in a timely manner, if at all. Manual processes are relied on to provide the glue between these siloed systems and this introduces errors because humans are not consistent.

Vigilance's own research taken from 5 years of client data and thousands of payment files has found through analysis of actual payment data, that 8% of creditor batch payment files and 9% of employee payment files used to instruct banks to make payments are incorrect. This is a staggering figure and is evidence that payment systems and processes are not as robust as expected.

Payment data isolated in different systems without centralised controls can add risk for an organisation. And makes it difficult to standardise procedures across multiple technology platforms. e-invoicing, when it becomes commonplace will help, but the human factor will still be the achilles heel. The Xero accounting platform has had e-invoicing for years yet very few use the feature, why?

While most of these erroneous transactions detected from our research will be human error, for example, duplicate payments or similar, the impact to the bottom line remains the same. However when it comes to payment fraud there is significantly more impact.

2. Exert taken from PWC online article: https://www.pwc.com/gx/en/services/forensics/economic-crime-survey.html

# Governance is the boards responsibility

Firstly there will be disruption to business. If the fraud was internal then there will be employment issues. As word spreads, and it will, the company culture can be impacted with staff mistrust, and customers, suppliers and shareholders will also have their own concerns. Questions will be asked about the systems, processes and governance (governance being the board's responsibility).

While many organisations will have fidelity insurance it can't protect the company's brand and reputation after the horse has bolted! It would pay to check any cyber insurance policy held as it may have an out clause for email compromises or other fraud scenarios.

The Auditor General's website[3] notes that a common misunderstanding is that a financial audit will detect fraud. While a financial audit will consider internal controls, it's not a forensic audit. A forensic audit usually takes place after a fraud has been detected to help determine the actual losses and method used to steal the money in order to prepare a case.

# Call the Police!

Determining the scale of loss from an internal fraud can be difficult and may never fully be uncovered. Going straight to the police with a complaint is likely to be met with frustration as the police need clear and concise evidence. The priority of blue-collar crime will take a backseat to more immediate and life threatening crimes. And while there is the Serious Fraud Office (SFO) they only have the capacity to take on a relatively small number of cases and most garden variety employee frauds won't meet their criteria. If you then need to bring in a forensic expert you are looking at more cost on top of replacing an employee in an already tight labour market.

Prevention is most definitely more cost-effective than remediation, and today we have technology to assist with prevention that didn't exist before; software that adds an extra layer of protection to your existing controls and ensures separation of duties. No board wants fraud on their watch. Avoid the expectation gap and ask some questions now and consider if your internal controls are really robust enough for today's fraud risks, it will save a lot of time and money and unwanted pain.

3. https://oag.parliament.nz/

# How do Boards manage a fraud event?

Many frauds are dealt with internally and swiftly, and there are a number of factors as to why. Most organisations don't know how to undertake an investigation or even want to, preferring to focus on daily business. However sweeping things under the carpet leaves unanswered questions affecting the culture of the organisation. Furthermore the offender could go on to new employment to reoffend. This is why fraud is so underreported.

Larger organisations who have Risk and Audit committees will be asked by the board how this happened on their watch and the investigation will be driven by that, often with external expertise. However Risk and Audit has a wide net to cast across the business and the expectation around the details of fraud protection processes will be considered the domain of the Financial Controller.

An initial police response, or facing hefty forensic investigation time and cost influence how to proceed. At the same time this is being considered there is the employment situation; not only replacing the person in question but also managing the exit of the accused.

Boards of public companies will probably be focused on damage control once a fraud is discovered and look to employ a PR firm to minimise brand damage. As already mentioned insurance can't cover brand damage or the impact on the organisations culture.

# Prevention is the best approach


Prevention is most definitely more cost-effective than remediation. No board wants fraud on their watch. Avoid the expectation gap and ask some questions.

- Who has oversight of the day to day payment processes and how robust are they really?
- Are our payment processes documented and are they being followed?
- What concerns do our payment approvers have when approving payments?
- What financial health and safety tools do we have in place for our Payroll and Accounts Payable team?
- How can the board assist the CEO and CFO regarding fraud review.

Today new technology is being adopted as part of the financial transformation to assist with prevention that didn't exist before; software that adds oversight to the existing systems and controls, ensuring separation of duties catching payment errors and fraud.

Consider what technologies can fill the gap. It will save time, money, reputational damage and a lot of unwanted pain.

# About Vigilance Ltd

A passionate team of entrepreneurs, developers, and professionals transforming how organisations manage payment security. Since 2012, our New Zealand based team have been developing products to assist a wide range of organisations with multiple business challenges across the areas of payment security and anti-money-laundering compliance (AML).

# About VigilantPay

VigilantPay is the flagship product of Vigilance Ltd. It has been developed to harness the power of cloud technology to aggregate an organisation's payment data for analysis from their, Accounting, Payroll and Banking platforms which are otherwise siloed from each other.

By centralising your payment data from the accounting, payroll and bank, analysis can take place in real-time during the critical approval process by automating cross-checks of proposed payments, which is not humanly possible to perform in a timely manner. These checks will surface any errors, unusual, or fraudulent payments prior to the bank being instructed to make payment, thus protecting the organisation from loss of funds and potential brand damage should fraud take place.

## Strength in numbers.

The VigilantPay platform not only provides protection by cross-checking an individual organisation's siloed payment data, it also uses advanced algorithms to cross-check against all organisations using VigilantPay by anonymised users payment data to ensure you are paying who you think you are paying.

VigilantPay's unique, yet practical, approach to protecting organisations from payment error and fraud attempts is a fit-for-purpose solution for today's high-risk online payment environment.

Today the VigilantPay platform is protecting billions of dollars for its users in real-time and importantly providing a solution that no other system can do on its own to protect an organisation from payments risk and the organisation's reputation.