The Growing Problem of Organisational Fraud (And How to Fix It)

Eyal Dushansky, Certomo

Yigal Newman, Ph.D. The Hebrew University of Jerusalem

You don't have to look long and hard to find the latest story of corporate fraud, embezzlement, or economic crime. It's an ever-present problem, and one that seems to be getting worse. David Smith from Florida, a former Diagnostics Manager, managed to get reimbursed for over $1.2 million in false expenses. He set up fake companies, created fake invoices and turned in fake expense reports for payments he'd supposedly made. At a Bookstore in North Carolina, Bookkeeper Anna Susan Kosak was caught for embezzling $348,975. Ms. Kosak was the only person managing the company books, she would write and cash, checks written out to herself.

In PwC's *2020 Global Economic Crime and Fraud Survey*[1], **47% of respondents** said they had experienced fraud in the past 24 months, the second-highest incidence rate in the past two decades. In the *Report to the Nation's 2020 Global Study on Occupational Fraud and Abuse,* CFEs estimate that their organisations **lose 5% of revenue to fraud** every year – that's equal to an estimated **$4.5 trillion globally**.

Prevention, as always, is better than cure. To hope that issues of fraud and embezzlement don't rear their ugly heads is to wait for the inevitable to happen. This is a problem that demands a proactive approach. In our experience, this approach is most effective when executed by the Chief Finance Officer or her Executive Finance team.

In this paper we will put the microscope on the twin issues of fraud and embezzlement – how they affect businesses large and small, and what a modern organisation can do to ensure it doesn't find its own name splashed across the finance section of the morning paper as the latest victim of economic crime.

Fraud and embezzlement don't discriminate

While the news might make it appear that fraud and embezzlement are issues restricted to large multinationals, the truth is that larger crimes are simply more newsworthy. These crimes occur in organisations both large and small. In fact, according to the *Report to the Nations*[2] study, a number of fraud risks are far more prevalent in small organisations than they are in large ones. In these "smaller" businesses, Billing fraud is 2x higher, Payroll fraud is 2x higher and Cheque and payment tampering is 4x higher compared to larger firms. While fraudsters may have less to gain from targeting a smaller organisation, their job is often made far easier by smaller firms that have neglected to put anti-fraud measures in place – a lack of internal controls contributes to nearly **one third** of frauds.

Why can't we rein fraud in?

With fraud and embezzlement such significant issues for organisations of all sizes, and with the problem seemingly growing larger year on year, the question has to be asked: why is economic crime so difficult to rein in?

There are three major obstacles that an organisation must battle against when fighting fraud.

1. It's difficult to identify

It goes without saying that fraudsters don't want to get caught. And with fraud tutorials just a Google search away, the task of identifying fraud sees organisations pitting themselves

---

[1] https://www.pwc.com/gx/en/forensics/gecs-2020/pdf/global-economic-crime-and-fraud-survey-2020.pdf

[2] https://www.acfe.com/report-to-the-nations/2020/docs/RTTN-Government.pdf

against the hive mind of the internet – a battle that is understandably difficult to win. Oftentimes an organisation will need help in identifying fraud: **43% of cases** are reported by a tip-off, with **half of those tip-offs** coming from employees.

2. It's difficult to prove

Given the consequences for getting caught, fraudsters are extremely diligent in covering their tracks. They know that any form of paper trail will greatly increase their chances of being caught, so go to great lengths to disguise their activity, make it appear legitimate, or disconnect it from themselves.

3. It's expensive to rectify

According to the Report to the Nation's 2020 Global Study, the median loss per fraud case is $125,000, while the average loss is $1.5 million – a skew in numbers that indicates the largest frauds are colossal. Naturally, many business owners perceive the cost of preventing these crimes to be as high, or higher, than the likely loss in the event of "regular", non-colossal fraud.

Be that as it may, when money is fraudulently being taken out of a company's coffers, it is left with fewer resources to devote to fixing the issue and preventing similar issues into the future. In our experience, if an organisation isn't careful in preventing fraud, this white-collar crime can become a self-fulfilling prophecy, with the effects of the last case laying the groundwork for the next. It's critical that you break the chain.

Larger multinationals face additional risk

While all organisations are at risk of fraud, larger organisations inherently face greater risks and greater consequences.

1. More bank accounts, more transactions, more opportunity

    Multinationals deal across geographies, with hundreds or thousands of suppliers and partners and potentially millions of customers. With so many bank accounts and transactions to monitor, this landscape can become a breeding ground for the misappropriation of moneys.

2. Operational complexity offers more places to hide

    Just as a multinational's external dealings become more complex as it grows, so too do its internal dealings. As operational complexity increases, it becomes easier for fraudsters to 'hide' within the organisation and quietly siphon off funds.

3. Forex markets create a smokescreen

    Organisations that deal across currencies face a far greater challenge in identifying fraud than those who don't, as forex fees and ever-changing rates can form a handy excuse as to why slightly less money than expected arrived at its destination, embezzlement is easier to hide in a fluctuating market of multiple currencies. Currency fluctuations can make it quite easy for savvy embezzlers to get a slice of each forex transaction, particularly in multinationals that deal in volatile and exotic currencies, as these often aren't as carefully monitored as major currencies are.

4. Costs are higher

    The more complex an organisation's accounting and finance systems, the more difficult fraud is to detect, and the more expensive it is to fix and prevent.

5. The bigger the name, the harder the fall

    Fraud often represents a significant hit to any firm's reputation – within the organisation, with creditors and shareholders, with customers and the wider community. The financial blow of the fraud itself often pales in comparison to the reputational damage it causes, as many stakeholders, suppliers and customers seek to sever ties with what they might deem a compromised business. Controlling this damage can prove incredibly difficult, as fraud makes for juicy news fodder, especially for multinationals, well known and recognized across the globe.

Having explained the underlying causes and effects, it's time to turn our attention to how might an organisation solve this growing problem.

How can fraud be detected and prevented?
Given what we now know, how might an organisation, multinational or otherwise, work to prevent instances of fraud and embezzlement?

As with any modern problem, technology presents several effective solutions, though they only form a part of a larger effort. You'll need to back the technology up with other strategies, including risk mitigation, training, governance, third-party management, candidate screening, and manually monitoring transaction processing. If you fail to take this multifaceted approach to combating fraud, you'll be far more likely to become a victim, and not just because a lack of process and procedures helps hide fraud in the clutter. Companies that choose to ignore these problems make themselves obvious targets to potential fraudsters - they're the lame deer in the herd that represents an easy kill. And without detection processes and with the fraudster sitting within your office perimeter, you could lose thousands, potentially millions, before the fraud is uncovered.

A modern problem requires a modern solution
It might feel counterintuitive to hear those instances of fraud are rising. Gone should be by now the days of cash and cheques being passed from hand to hand – every finance process has and should be digitized, meaning that every transaction should be recorded. But it is here where fraudsters see opportunity – a modern multinational is now faced with almost too much financial data, allowing fraud to be hidden within the endless zeroes and ones. Reducing fraud is often a simple matter of reducing complexity. Streamlining your accounting and finance practices reduces the number of places a fraudster can hide. In this way, global cash management can offer an effective solution to multinational fraud.

Trading slow and manual for instant and automated
Humans are great at a lot of things, but processing endless data isn't one of them. Happily, that is one thing that technology is great at. Many multinational organisations are currently using rather inefficient accounting and finance systems that make them far more vulnerable to fraud. These systems:

- Are often drip-fed information in a disorderly way (data might come daily, weekly or monthly from different banks, transactions from different regions may be uploaded on different schedules.) This is causing more damage than benefit.
- Often task humans with manually pulling together this (already outdated) information, by applying endless hours of "data cleansing".
- Simply display the information as it comes in, with limited analysis and reporting functionality.

An organisation is thus left with an incomplete and/or an inaccurate picture of its finances based on data that might be a day old in some parts, and weeks or months old in others. This mismatch in timing may help hide frauds, by prompting the humans overlooking the data to ignore red flags because "the next batch of data will sort this out". Of course, by the time the next batch of data arrives, it includes more issues that will be ignored for the same reason, and so on.

Global cash management systems - otherwise known as treasury systems, liquidity management systems, and cash and risk systems - represent the evolution of multinational finance. The best will:

- Aggregate all relevant information online, pulling the data directly from banks in real time.
- Use algorithms to make the data uniform and present it in a digestible, meaningful and contributing way.
- Offer an almost real-time view of a multinational organisation's finances.
- Allow for easy reporting and analysis to better identify the irregularities that so often point to fraud.
- Instantly and discreetly notify senior people of any suspect transactions.

These systems use machine learning to become ever better at identifying fraud. If they detect pattern that points to fraud, this pattern is added to the screening algorithm, ensuring any similar cases are picked up in the future. No matter where and when the fraud took place, what language, country, or currency it was in, the fraudster and their methods are shared across all organisations, ensuring the same strategy can't be used again. Global cash management systems seek to transform a multinational's greatest vulnerability to fraud – endless financial data – into its greatest strength. Rather than being able to hide within the zeroes and ones, fraudsters will instead circle themselves in red ink, as constantly evolving algorithms use data analysis to put a spotlight on irregularities.

Technology is only as good as the systems that surround it

While technology is becoming better and better at *identifying* potential instances of fraud, *acting* on that information is up to you. According to PwC, **6 in 10 organisations** don't have a program to address bribery and corruption risk, and **barely half** are dedicating resources to risk assessment, governance and third-party management. We revealed earlier that a lack of internal controls contributed to **nearly one third of frauds**. While internal perpetrators (37%) account for slightly fewer total frauds than external perpetrators (39%), they account for far more at the upper end: **nearly half** of reported incidents resulting in **losses of US$100 million or more** were committed by insiders.

All this is to say that technology will only take you so far. In order to effectively fight fraud, an organisation needs to take a more comprehensive approach that includes the following strategies:

- **Risk assessment and mitigation:** All fraud risks should be identified, prioritized, and addressed. The fraud landscape is in a constant state of flux, so robust risk assessments should be conducted regularly across departments and geographies.
- **Governance and monitoring:** Make a person or team responsible for ensuring fraud policies are defined, fraud procedures are sound, and your organisation is constantly monitored for potential instances of fraud.
- **Training and reporting:** Perhaps the best weapon against fraud is education and exposure. If you're open about your efforts to combat fraud, and if you educate your employees on what to look out for, you're far less likely to become a target. If fraud does occur, you'll also be in a far better position to catch it, as fraud awareness training makes employees over **50% more likely** to use formal fraud reporting mechanisms.

Part investment, part insurance

Given the above, it's evident that fighting fraud demands real and ongoing investment, in terms of technology and strategy, money and time. Unfortunately, this hurdle is where many organisations tend to fall. **Less than 30%** of PwC survey respondents strongly agreed that they had been able to successfully implement or upgrade their technology, citing high costs, low resources and a lack of the supporting systems described above.

The fight against fraud and embezzlement cannot be seen as a cost. It should instead be viewed through a pair of equally critical lenses:

- **As an investment:** By committing resources to fighting fraud, you're making a meaningful investment in your organisation. Such a commitment strengthens your reputation, instils trust within your team, and generates stakeholder, supplier, creditor and customer confidence. While the return on this investment may not be delivered as a dividend or a payout, the value of the frauds such an approach will avoid could comfortably count in the millions.
- **As insurance:** As we said at the top, prevention is always better than cure. The technologies and strategies discussed above form the most effective fraud insurance policy there is – one that doesn't cover the costs of economic crime, but that prevents those costs from being incurred in the first place.

By shining a light on fraud, you go a long way to preventing it. That's our philosophy at Certomo, which is why we've developed a global system, designed to remove the shadows in which fraud so often lurks. For example, we have taken the 150 years old Benford's law, enhanced it and adapted it to the reality of global transactions in the 2020s. This technique, with others, allow us to assist today's Finance teams to identify fraud within their organisations. Reach out to us at Certomo to see how we may be able to assist your organisation as well

Certomo is an online SaaS application that provides treasury and cash finance teams real-time, AI-driven finance management capabilities such as cash and liquidity management, global account aggregation, vertical supply chain financing and proactive internal fraud and embezzlement monitoring. Certomo's cloud-based service can be used anywhere in the world, can connect to any bank, can be analyze with any currency, and can be managed in any language.

Dr. Newman is the head of the FinTech Program at the Hebrew University Business School, where he reaches FinTech and Finance courses. He also advises to various FinTech companies.