qLegal

The small print for BIG IDEAS

Disclaimer: This publication describes the law in general terms. It is not intended to provide legal advice on specific situations and should not be relied upon as a source of legal advice.

Date produced: 9th July, 2021

qLegal Online Publication

Protecting your start-up from fraud.

This online publication explains how you can protect yourself from different kinds of fraud.

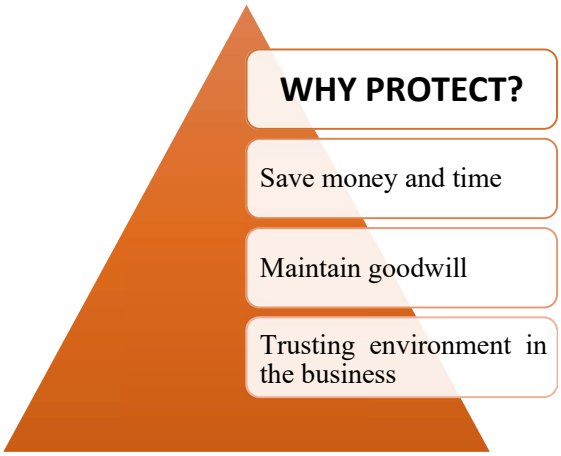
There has been an increase in both instances of fraud and the amount of money that is lost due to fraud. The easiest targets are start-ups because they are in their initial stage of development with few staff resulting in less supervision and a work-in-progress security system. This can adversely affect the growth and success of the business. In this paper, we will discuss the importance of protecting your start-up, potential parties who could commit fraud and what steps need to be taken to protect your start-up from fraud.

Why is it important to protect your start-up from fraud?

It is important for you to protect your start-up from fraud for the following reasons:

1. To prevent loss of money from your business. While it may seem burdensome and costly to put in place a robust security system, it will definitely save you a lot of money in the long run as well as time. This is because you won't have to later spend time in resolving the issues relating to fraud.
2. To build and protect the goodwill in the business. A start-up has to invest a great deal of time in developing its unique selling point, differentiating itself from its competitors and forming positive relationships with customers and suppliers (which includes demonstrating that it can be trusted). Any allegations of fraud within or occurring to a start-up can be a huge hindrance in its success and can affect its reputation.
3. By having in place effective strategies to prevent fraud, it will also encourage staff to be more truthful and promote open communication. If any new staff member joins your

start-up, they will know from the beginning that insincere behaviour will not be accepted.



Who could commit fraud against your start-up and how?

1. Internal staff: While staff members tend to be considered as trusted assets of a business, the sad reality is that sometimes these same staff members can be responsible for committing fraud. Such behaviour could be because of greed, unsatisfactory work environment, immediate need of funds for personal reasons, etc. Some examples of fraud that could be committed by staff members include:

    - Payroll fraud: This is where a staff member lies about the number of hours that they have worked by manipulating the time entered in their timesheets and thereby giving the impression that they should be remunerated more than what they are really due. A staff member may also involve other staff members to help them by asking them to sign-into their work account on their behalf when they aren't really at work.
    - Asset misappropriation: This is where a staff member might try to extract money either directly from the customer or business by forging checks or misappropriating the inventory or accounts of the business. This will also include

fake invoice fraud where a staff member creates invoices which are not genuine in order to steal money from the business.

- Data leakage: This is where a staff member might leak sensitive information about the business to a competitor or third party which could damage the reputation of the business.

2. Customers: A business serves and is constantly dealing with customers, so unfortunately there are many opportunities for businesses to be defrauded by their customers. Fraud by customers arises because of the customer's need or desire to receive goods or services without paying for them. Some examples of this type of fraud are:

    - Payment fraud: This happens when the customer tries to make the payment through counterfeit money or stolen debit/credit cards.

    - Charge back fraud: The customer purchases the product online via their own card and then disputes the payment with the bank after receiving the product.

    - Return fraud: Very often, customers purchase a product, use it and then return it even though the product is in perfect condition. For example, people purchase products from European countries with tax exemption and then return it in a third country where the taxes are applicable. Another form of return fraud is when a customer might steal the product and try to return it to make some money out of it.

3. Suppliers: Start-ups tend to be very careful with their suppliers but over time and as they scale, there may be several members of staff engaging with different suppliers, and these members of staff may accidently open themselves up to fraud. The suppliers might start to over-charge or supply lower quality goods or services due to complacency or a belief that the start-up won't notice. Some examples of fraud concerning suppliers are:

    - Billing fraud: The supplier might provide false or inflated invoices to the business.

qLegal
The small print for BIG IDEAS

- Quality assurance fraud: The supplier might guarantee a certain quality of the product but sell the one with lower quality.

4. Other third parties: The last category is people who are not connected with the business but try to extort money by illegal practices. Some examples of fraud occurring in these situations are:

    - Counterfeit products: Hackers/scammers might try to sell counterfeit products of the business. For such hackers/scammers, start-ups are easier targets because they are new and have covered a smaller market area.

    - Stealing information: Scammers might try to install software into the business systems and gain access to sensitive information or even block the systems in exchange for money.

    - Social engineering: Imposters might try to extort money from staff by posing as high-level officials of the business.

How can you protect your start-up against fraud?

Fighting fraud is a team effort, therefore it becomes the responsibility of each member of the business to recognise the fraud. Education is the key to protect both the business and its staff from any kind of fraud. Here are some ways to protect your start-up against fraud:

1. Know your business:

    - Every person should know how to conduct and secure the business.

    - Educate every staff member regarding how to deal with online fraud, to know when fraud is happening and what steps to take to prevent it.

    - Conduct proper staff background check to know your staff.

    - Keep all electronic devices password protected; there should be a policy for everyone to change their passwords every 30-45 days.

Senior management within a start-up should know in detail about the finances and operations of their start-up. The chances of fraud happening within a start-up is high and commonly happens by way of staff members embezzling money. Therefore, it is important to keep an up-to-date check on financial books and records and the staff members that have been entrusted with the day-to-day responsibility for making payments.

2. Do appropriate external due diligence:

   - Carry out external due diligence at the onset of every business relationship and at a minimum on an annual basis, conduct an internal audit that ensures that within the company there is a full understanding of the controls in place.

   - Due diligence should include financial, operational, legal, compliance and reputational analysis. It can be conducted, for example, by engaging with a supplier for more information on it and conducting independent research on the supplier concerned. This should be part of the periodic KYC (Know Your Customer) review.

There are different ways to ensure security controls to avoid fraud. There are two initial steps that start-ups should immediately set up to prevent and maintain a framework of safety against fraud:

1. On an annual basis (at least) conduct a Fraud Risk Assessment: through this exercise, the start-up should identify the risks they are exposed to (is the business vulnerable to cyberattacks? Is it necessary to separate areas of the start-up to ensure no information contamination between, for instance, the public and private side of the start-up?). This way, the start-up, looking at the previous year's concerns, regulatory changes and market situation, will be able to update its risk map and be able to implement controls of both a preventive and a detective nature.

qLegal

The small print for BIG IDEAS

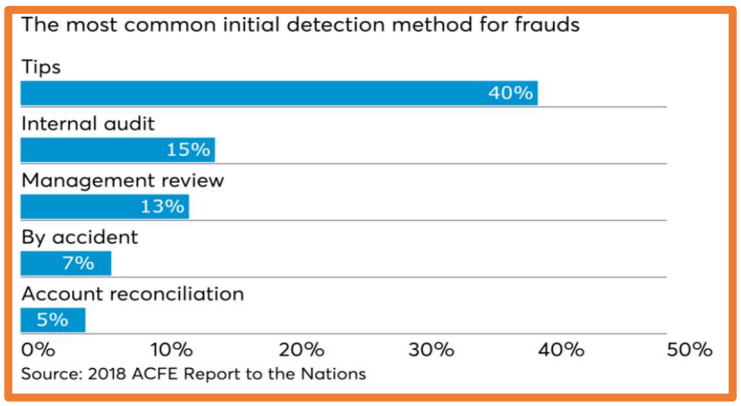
2.Monitoring the results of the Fraud Risk Assessment will be key to identify the potential circumstances for when there may be a risk of fraud occurring. Fraud detection and monitoring should be set up depending on the vulnerabilities identified when conducting the Fraud Risk Assessment. As data, traditionally, has been one of the targets for fraudsters, we recommend that you consider and document the data flows in your business (as required under data protection law) and closely monitor certain data flows (such as payment and transaction data). The Fraud Risk Assessment should be completed by senior management within the start-up who are familiar with finance, operations, and IT.

The following are free methods for a start-up to prevent fraud and provide a safer environment:

- create password protected folders that only designated members can access - for example, it is strongly recommended that folders containing staff members' information are only accessed by the other staff on a need-to-know basis;

- when it comes to payments for the start-up, a four-eye check-up system so that payments are being reviewed and approved by two staff members (ideally the founder and the team member responsible for the finance of the start-up, someone who might have an independent role within the staff if possible); and

- for contractual obligations, start-ups need to review their framework on with whom and how the start-up engages in contracts. This is particularly key for suppliers and third parties to ensure that the processes are done in a transparent way.



qLegal

The small print for BIG IDEAS

All the measures that a start-up implements to avoid fraud need the cooperation of the staff. The staff are the ones who can see, identify, detect, investigate and escalate if something does not seem quite right.

Through internal training (provided by a compliance officer, or general legal training, or someone else at the business or through external training provided by a third party business), staff members need to be regularly communicated to and trained on not only the different forms fraud can take but also how to escalate a potentially fraudulent situation in an appropriate way.

The start-up could consider providing its staff members with an independent, appropriate person to whom to escalate any fraud concerns and needs to ensure that staff members have a safe way to provide information that is of concern without fear of any negative repercussions.

Conclusion

Start-ups need to consider fraud as a highly likely threat and not an abstract concept. By identifying the needs and risks of the start-up, methods can be put in place to prevent, detect and avoid fraud. Regardless of the stage your start-up is at, it is never too late to ensure safety and protection against fraud.

Other Helpful Resources

Please also review qLegal's online publication *Protecting Your Start-Up from a Cyberattack,* available on the Resources page of the qLegal website:
http://www.qlegal.qmul.ac.uk/resources/

This online publication was drafted by LLM students participating in qLegal, the pro bono commercial law clinic at the Centre for Commercial Law Studies, Queen Mary University of London: Radhika Goel, Prerna Negi and Anabel Victoria Martinez Mari De Haas.

qLegal provides free legal advice and resources to start-ups and entrepreneurs on intellectual property, data protection, corporate and commercial law. See http://www.qlegal.qmul.ac.uk/ *for more details and to book your appointment now.*