CORPORATE IDENTITY FRAUD: A PRIMER

Hanim Norza Baba, Head of Graduate Studies Center, Universiti Teknologi MARA, Melaka, Malaysia.
drhanimnorzababa@gmail.com

ABSTRACT

Corporate identity fraud occurs when someone gains access to sensitive information relating to a businesses and uses it to deliberately misrepresent the businesses's identity. Corporate identity fraud can be as simple as stealing a corporate logo or as severe as assuming the identity of a major corporation. It can result in significant financial loss, paralyse business operations or cause substantial damage to the businesses's most valuable asset – its brand. Once you have become a victim of identity fraud it can be difficult to recover any lost money and impossible to get back the time spent clearing your good name. Many victims continue to have issues with their credit rating years after the incident, proving a nightmare when applying for mortgages and loans. Understanding the risks and taking some simple steps can help prevent you from becoming a victim of identity fraud.

Keywords*: Corporate Identity Fraud; Risks; Prevention*

Introduction

Identity fraud involves the use of an individual or a business's identity information to open bank accounts, obtain payments or credit, fraudulently obtain social security benefits (in the case of individuals) or obtain goods and services. The types of identity fraud are businesses hijacking[1] and businesses impersonation.[2] Accordingly, corporate identity fraud (CIF) can be defined as the abuse of traditional and non-traditional identity assets with the intent to divert, deceive or defraud consumers (Fite, 2006). CIF (also known as business identity theft, corporate or commercial identity theft) is a form of identity theft in the criminal enterprise. CIF occurs when a false corporate identity or other businesses' identity details are used to support unlawful activity. A criminal can change the corporate registration information of a business, such as altering the names of the corporate officers, and then use the business's corporate registration history along with additional false documents to establish lines of credit with banks or retailers. Identity thieves can then purchase items that can be bought and exchanged for cash or sold with relative ease. The damage can be devastating to both the entity that had the unauthorized change to its corporate information and the bank or retailer doing business with the corporation. The damage to the business entity's credit history can lead to denial of future credit or simply increase the cost of future borrowing for that entity, which can lead to operational problems.

Corporate Identity Fraud

The term 'corporate identity fraud' is commonly used to describe the impersonation of another organisation for financial or commercial gain. CIF occurs when someone gains access to sensitive information relating to businesses and uses it to deliberately misrepresent the businesses' identity. CIF can be as simple as stealing a corporate logo or as severe as assuming the identity of a major corporation. It can result in significant financial loss, paralyze business operations or cause substantial damage to the businesses' most valuable asset that is, brand.

Further, it is not just individuals who can fall foul of fraudsters; the businesses can also have their identities stolen too. Corporations are being targeted by ruthless criminals who can use their identity to trade off the real businesses' good name to obtain goods and services on credit from suppliers. Fraudsters set up a false businesses to trade or steal the victim organisation's identity and/or financial information and use it to purchase goods and services, obtain information or to access

[1] For example, a fraudster submits false documents to Businesses Commissison of Malaysia (CCM) to change the registered address of your organisation and/or appoint 'rogue' directors. Goods and services are then purchased on credit, sometimes through a reactivated dormant supplier account, but are never paid for.

[2] For example, a fraudster impersonates your business to trick customers and suppliers into providing personal or sensitive information which is then used to defraud them. Your business may be impersonated using phishing emails, bogus websites and/or false invoices.

facilities in the organisation's name. However, this is not the only area of risk. Fraudsters can obtain signatures from public records and attempt to attack businesses bank accounts by purporting to be the signatory on the account. If the victim corporate identity is stolen, it could face considerable hurdles including correcting public records, repairing credit ratings and rebuilding confidence with suppliers and customers.

All businesses are at risk. Therefore, awareness of high-risk areas can assist in developing cost-effective controls to protect against fraud (Albrecht and Schmoldt, 1988). However, those with less developed controls on information security are more vulnerable. Once false information has been filed with Businesses Commission of Malaysia (CCM), fraudsters can use a businesses' corporate identity to obtain goods and services on credit that are never paid for, or even trade on the good name and reputation of the genuine businesses.

How does the fraud work?

A fraudster steals or acquires information about victim organisation. This may include the organisation' s name and businesses number (if incorporated), the address of the registered office, the information relating to the directors, employees or customers, and details of the supplier accounts. This information is then used to acquire financial products for example, loans and corporate credit cards, order goods and services on credit, hijack businesses bank accounts, deceive customers, and purchase assets. Sometimes a fraudster will change the business's details for example, the directors' name or registered address with CCM in order to facilitate the criminal activity. Alternatively, a fraudster may simply set up a false businesses to purchase goods and services on credit from victim organisation and disappear before paying for them. Also, organisations can be vulnerable to corporate identity fraud committed internally by employees, externally by individuals or organised criminals, or in collusion.

Business or corporate identity theft occurs when a thief uses an existing business' name to obtain credit, or bills a business's legitimate clients for products and services. Often, but not always, Personal Identity Card or Employer's Identification Numbers is required to commit business identity theft. These numbers are readily available in public records, dumpsters, or internally, and the relative ease of access to these identifiers facilitates this crime. Business identity theft takes many forms. Posing as a look-alike or sound-alike business to lure customers is one of them. In many cases, shady operators go after information to tap into business' credit and reputation. For example, they change a business's contact information and then use it to obtain credit cards or order goods, skipping town before bills arrive. Perpetrators of business identity fraud are often employees or former employees with direct access to financial documentation (Sicilliano, 2012). They have the opportunity to pad the books in favor of their scheming. Victims of business identity theft often do not find out about the

crime until significant losses accumulate, or someone discovers discrepancies on the books. Because of the hidden nature of the transactions, businesses can lose vast amounts of money. Business identity theft can remain undetected for years.

What happens if business becomes a victim?

Once the organization becomes a victim of identity fraud, it can be difficult to recover any lost money and impossible to get back the time spent clearing your good name. The cost to clean up and correct the damage can reach hundreds to thousands of dollars and hours of lost time. Many victims continue to have issues with their credit rating years after the incident, proving a nightmare when applying for mortgages and loans. Understanding the risks and taking some simple steps can help prevent the organization from becoming a victim of identity fraud.

Corporate identity fraud can have a financial and reputational impact on the organisation. Rectification need to be done about the damage caused by the fraudster (particularly to credit rating) and this can take time. Among the prevention steps are report the matter to the police and other relevant organisation(s) immediately (eg, suppliers, CCM) and follow their advice, inform the customers if their details may have been compromised or a fraudster may have contacted them as a 'representative' of the victim business, obtain copies of the organisation's credit report (available from credit reference agencies) and CCM record and check for discrepancies. Then, keep a record of all correspondence make or receive in respect of the corporate identity fraud and reassess the organisation's risk management and control systems to ensure that the business is adequately protected.

How to protect the organisation?

Resolving issues caused by business identity theft can be a time-consuming and challenging process. Businesses should have comprehensive security strategies in place. If we own the business or are responsible for running a business, corporate identity fraud is a threat that we simply cannot afford to ignore. The most efficient ways to prevent identity theft is with an identity theft protection service and a credit freeze. It is vitally important to do all the things a consumer would do to prevent identity theft such as shred documents, get a locking mailbox and make sure your network is secure. There are many steps you can take to help minimize the risks including confidential shredding of sensitive data. When information is no longer required, it must be securely destroyed. Shredding information is the best way to dispose of documents securely and to ensure that criminals cannot gain access to sensitive businesses details fraudulently. Cross cut shredders provide greater security by cutting paper into small confetti-like particles and also reduce bulk waste.

Besides that, look after the corporate identity. Many of the rules that apply to individuals can be adapted to protect businesses. Businesses can and should put measures in place to reduce the opportunities open to criminals to commit identity fraud and to use their organization for criminal activity. Do regular check-up the registered details of the businesses and its directors thru CCM. Cross-reference and validate CCM information with other independent sources of information, such as trade associations, professional bodies and trusted internet sites. Remember that fraudsters can easily set up internet sites to back up their claims. Consider the information about the businesses that exists in the public domain. In particular, try to avoid showing unnecessary information on headed paper or websites. For example, we need to place your businesses number on invoices, and then there is no need to put this on headed notepaper. If we need to advertise the appointment of a new member of staff in the press, limit the amount of personal information so that fraudsters cannot abuse it. Also, be wary of invitations to take part in business prize draws, as these can be an easy way for fraudsters to obtain potentially useful data on employees and the organization. Similarly, the victim businesses can become a goldmine for fraudsters if the information is not protected. The information need to be protected starting from setting up a credit card or credit account in the businesses name to get goods and services which ultimately need to pay back. Criminals can trade off the back of the real businesses's good name or obtain signatures from public records and attempt to attack businesses bank accounts by purporting to be the signatory on the account.

Regarding the documents procedures, having a well formulated document disposal policy in place, and adhering to it, is the first crucial step in protecting the business from corporation identity fraud. Define clearly what the management mean by sensitive or confidential information and make sure that anyone who handles or has access to this information knows how it should be saved, stored and ultimately destroyed. Also, need to include electronic media as well as paper in the guidelines. The staff also need to be caution about the risk of giving out businesses information online or over the phone without first checking to whom they are giving the information to. As part of the security policy, the businesses should implement guidelines on what personal information should be divulged to third parties, particularly by electronic means such as email. Continuously do regular check-up on the registration details at CCM, bank details and website for any unusual transactions or discrepancies. Businesses must be responsible for ensuring that firewall and antivirus software is kept up-to-date. This way staff can securely open legitimate email attachments for viewing. Businesses also have responsibilities beyond the protection of their own identity. Organisations of all sizes are responsible for safeguarding the identities of their employees and customers and ensuring that their identities cannot be stolen and used by criminals. Businesses need to make sure their employees understand the risk of identity fraud to the business, the customers and to themselves and their families.

Businesses also can introduce a clean desk policy, where this reduces the risk of identity theft in the workplace as passwords and confidential information gets locked away. - From small retail outlets to large corporations, all businesses are responsible for the protection of their customers' data. Also, need to understand your systems that to know what personal information you have in your files and on your computer. Understand how personal information moves into, through, and out of your business and who has access or could have access to it. For example if you are a retail outlet, make sure you follow the rules and regulations regarding abandoned credit card receipts. Another aspect, minimise what you keep that is, keep only what you need for your business. These days, if you don't have a legitimate business reason to have sensitive information in your files or on your computer, don not keep it, shred it and bin it.

Also, keep data secure and organised well and protect the information you keep. Be cognisant of physical security, electronic security, employee training, and the practices of your contractors and affiliates. Lock away sensitive documents in a safe place and limit access to these documents to the staff who really need them. Draft a plan to respond to security incidents. Designate a senior member of your team to create an action plan before a breach happens. It is also vital to promptly pass along information and instructions to employees and customers themselves regarding any new security risks or possible breaches.

Conclusion

Even if you're doing everything right to protect yourself from identity theft, the challenge with breaches is that they come from third-party organizations. Although we all expect them to handle our personal information discreetly and with a high degree of security, the breaches we hear about all the time are certainly cause to wonder how secure our identities really are.

References

Fite, B.K. (2006). Corporate Identity Fraud: Life-Cycle Management of Corporate Identity Assets. SANS Institute InfoSec Reading Room. *www.sans.org/.../**corporate-identity-fraud**-life-cycle-ma... - United States*

Whitlock, S, and Campbell, M. (2008). Corporate Identity Fraud. www.fraudadvisorypanel.org

Sicilliano, R. (2012). What Is Business or Corporate Identity Theft? http://www.infosecisland.com/blogview/21326-What-Is-Business-or-Corporate-Identity-Theft.html

Kemp, B.P. (2010). Corporate ID Theft. http://sos.ga.gov/corporations/idtheft.htm

Albrecht, W.S. and Schmoldt, D.W. (1988) Employee Fraud, Business Horizons, July-August: 16-18.