

Identity Theft, Consumer And Brand Fraud: You Are Targeted!

Introduction

In a thriving economy with freer exchange of goods and services, the 'new electronic marketplace' has exposed us to novel and unseen threats and crimes, affecting consumers and businesses alike; namely identity theft, consumer fraud and brand falsification. The latter alone, brand falsification, has accounted for 5-7% of fraudulent world trade, costing the global economy \$650 billion in 2008.

At this stage, it is critical to raise awareness in Egypt concerning the dangers associated with personal data theft, fraud and violation of Intellectual Property Rights (IPR), so that individuals, businesses and the government take the necessary precautions to enjoy the benefits of open markets and technological advancement while simultaneously avoiding the pitfalls of a globalized world economy. Aware of the fact that to protect its own interests, the business community is in dire need of a better informed and educated consumer, as rightly asserted by Mr. Gamal Moharram, AmCham President and Chairman of MGM Financial and Banking Consultants, the Trade-Related Assistance Center (TRAC) at the American Chamber of Commerce in cooperation with the Consumer Protection Agency (CPA) hosted on June 15, 2009, a conference on consumer protection. The conference was titled 'Identity Theft, Consumer and Brand Fraud: You are Targeted!' In his inaugural address, H.E. Minister Rachid Mohamad Rachid, Minister of Trade and Industry, stressed that since the said fraudulent activities do occur in Egypt, and have become easier to commit through today's spread of internet, mobiles, credit cards, etc, there is an urgent need to forcefully counter these acts, which he views as criminal, primarily through increased awareness, communication as well as just and fair penalties. He stressed that neither the government nor business can afford to lose consumers to theft or fraud. The conference featured a panel of prominent national and US experts who shared their experiences and first-hand knowledge as to how and why these crimes are orchestrated and how Egypt and the US can learn from each other's experiences in order to overcome these breaches and prevent their proliferation in both markets.

This report is divided into two major parts, the first deals with consumer and brand fraud and the second with identity theft. The first part, addresses sequentially the effects of fraud on consumers and businesses, and takes the Procter and Gamble experience in Egypt as a case study. The second part of the report devotes itself to the wide-ranging effects of identity theft as a relatively recent phenomenon, and takes Microsoft and HSBC's prevention activities in Egypt as practical examples to protect consumers and businesses. This report will then recommend specific actions by individuals, businesses and the government, concluding that in order to achieve success in countering these fraudulent practices there is a need for further collective effort between the different stakeholders, and increased awareness-raising at all levels.

I. Consumer and Brand Fraud

I.1 What is Fraud?

Counterfeits, look-alikes, pirated products, unauthorized service products and products that fail to provide certain functions are deceptive products characteristic of brand fraud. Consumer fraud is when a business misleads consumers into purchasing counterfeit goods or services by marketing them as genuine, or accepts payment for goods/services that are then never delivered. These and similar practices are all labeled fraudulent since they are all deceptive, put consumer health and safety at risk, devalue brand equity, and threaten legitimate brand owners and businesses.

Fraud can evolve from the use of numerous everyday items such as pharmaceutical drugs that can result in death or other health-risks; shampoo that can make your hair fall out; electronic products that can cause fires; sunglasses without any UV protection that could harm your vision; or baby formula without any nutritional ingredients. These are but a few examples of fraudulent and counterfeited goods that pose grave threats to the health and safety of consumers. These items are often difficult to detect and usually only identified after the damage is already done.

I.1.a Consumers are the first victims

Assessing the impact on the consumer of counterfeit pharmaceuticals, which are major violations of intellectual property rights, it is clear beyond any doubt that these products are a great danger to public health and safety as they may contain no active ingredients, have an incorrect amount of active ingredients, contain harmful ingredients, or have completely different active ingredients to the ones listed on the label. Such a deception can cause death or other health-related risks for the consumer. According to Mr. J. Todd Reves, Attorney-Advisor, US Patent and Trademark Office, US Department of Commerce, the dilemma is that sometimes consumers might be totally unaware of their consumption of counterfeit drugs, as these products can be sold in legitimate pharmacies due to a system of open distribution. Although pharmacies try to guard against stocking counterfeits, there is a weak link between pharmacies and the drug producers, which forces drugs to be transferred through many different entities before reaching the pharmacy. According to the WHO, 10% of all drugs are counterfeited, and 30-40% of all drugs in developing countries are counterfeit. Counterfeit pharmaceuticals are then a widespread crime against IPR that is difficult to detect and directly impacts the consumer.

Consumers' health and safety is also frequently jeopardized by various deceptive claims that provide a misrepresentation of reality, as explained by Ms. Sara De Paul, Attorney, US Federal Trade Commission. An 'extraordinary claim' stating that a cure for cancer has been found in the form of a vitamin sold on the internet is one such example. It is highly unlikely that the claim to have a cancer curing vitamin is true since researchers have long struggled at great expense to obtain such a cure. Even if true, a cure for cancer would not be cheap and obscure, nor would it be sold online. 'Quick and easy' claims are also

misleading and usually detrimental to consumers. It is highly unlikely that e.g. pills can effectively and safely help a consumer lose weight without a special diet or exercise. Buying into such claims will directly or indirectly harm consumers by preventing them from seeking valid cures for their ailments. Although 'no-risk guaranteed' claims may be true; generally such products/services are sold through some level of deception.

I.1.b Businesses are not spared from fraud

Although the extent of the damage is difficult to surmise, the impact of these types of crimes on businesses and economies is a loss of revenues worth hundreds of billions of dollars as well as a reduction in the will to innovate and the ability to attract FDI. Goods and services sold through deception and unfair practices divert sales from honest businesses and strain their ability to compete in the market. In New York City alone, \$1 billion in revenues is lost annually to counterfeit and pirated sales. As China produces more than 85% of all counterfeited goods that flood the US and European markets, it is evident that IPR-based businesses and investment in critical R&D in these markets suffer. A loss of financial returns leading to a lack of enthusiasm for technological improvement or cultural production clearly has long-term consequences for national economies, as well as the global community.

The magnitude of these negative impacts makes it incumbent on governments and businesses to fight fraud with all their strength. This is, however, easier said than done as these crimes have become highly lucrative and very hard to stop. The commercial advantages enjoyed by criminal enterprises are immense. For example, Mr. Reves affirmed that pirated DVDs, music and business software generates an estimated 800% profit with minimal risk of imprisonment – as opposed to illegally smuggled heroin, which generates far lower profits ranging up to 400% with penalties reaching life imprisonment. Although there have been improvements in the seizure of counterfeit products, the total US domestic value of seized goods increasing from \$125 million in 2006 to \$200-220 million in 2008¹, these crimes are far from being successfully contained. As long as the margin of profit continues to grow and the perpetrators continue to face low risk of penalization, there will be no end to the adverse effects on economies and businesses. While authorities struggle to keep up with the growing phenomena of fraudulent crimes, criminal enterprises continue to earn high profits, with minimal risk of prosecution.

The success of fraud and counterfeiting is also enabled by consumers who respond to their immediate needs and desires for cheap goods and services. Mr. Reves stated that it was found that many consumers in the United States believe that intellectual property rights crimes are a low-priority issue, limited to lost profits for wealthy corporations. Some consumers believe there is no reason to pay full prices for goods that will be matched with newer products within a short time span. They would rather own counterfeit designer handbags at a small percentage of the retail cost, cheap technology that will be outdated within a few months, or even counterfeit shoes for a fraction of the

¹ Combined statistics from the US Department of Homeland Security, Customs and Border Protection, Immigration and Customs Enforcement

cost. According to Saeed El Alfi, Chairman of the Consumer Protection Agency, the greater problem is when consumers are successfully deceived to think they are purchasing authentic goods, when in reality they are counterfeit, IPR theft goes beyond economic harm for businesses and luxury designer goods, when undetected, counterfeit goods put the health and safety of the consumer at risk.

I.2 How is Procter and Gamble (P&G) Egypt reacting to the counterfeit market?

Beyond the financial losses of approximately \$1 billion each year worldwide, the growing counterfeit market has also threatened the reputation of P&G brands and the company itself. The most common counterfeits experienced by P&G fall within the categories of powders, shampoos and imported counterfeits, Mr. Mohamed Sultan, General Manager, P&G Egypt stated in his presentation.

Counterfeit shampoos have been a large-scale problem for P&G. According to research conducted in Egypt, it was found that people had access to used original bottles, notably from the garbage area of Mokattam. On the basis of this research, P&G Egypt commenced the Mokattam School Recycling Project in 2000; which garnered the support of many individuals, international organizations and companies. This project, which engaged with Mokattam locals to get them to collect disposed bottles from the trash and recycle them, has been instrumental in reducing counterfeit hair care products. Through teaching environmental responsibility, the school was simultaneously reducing the impact of the counterfeit business on P&G. Through P&G's efforts, the school began to recognize particular techniques of counterfeiting, and became an additional source of information for P&G Egypt. The project managed to collect approximately 1 million bottles—1 million bottles less of counterfeited products. The 150 children directly involved in the project have benefited in many ways; they are making money per bottle collected, improving their math skills as they calculate how much they are earning per bottle, and they are improving their computer skills as they electronically document their findings.

Given the large-scale of this issue, this example depicts how P&G Egypt took a multi-pronged approach to address the problem of counterfeits. They provided incentives for retailers to refrain from dealing with counterfeit products and united forces with others in order to have a strengthened collaborative effort that yields better results than the company could on its own.

II. Identity Theft

II.1 Ease of Identity Theft

Identity theft involves the theft and usage of another's personal data in order to pose as that person, to conceal one's true identity from government and law enforcement authorities or others who perform background checks, or to fraudulently obtain goods or services in the name of another individual. It is becoming a widespread global phenomenon largely attributed to the new electronic marketplace, which has facilitated enhanced access to personal information for thieves all over the world. Thieves generally

make use of stolen identities for financial gain or concealment. In 63.5% of identity theft crimes a credit card has been the source of personal data. Mr. El Alfi stated that in 2008 in the US alone, there were 9.9 million victims of identity theft; an increase of 22% over 2007.

In the past, for a person to commit a crime against another, they both had to be physically present in the same place; today this is no longer the case. Now, it is much easier to become a victim of a crime, particularly identity theft, without even realizing it until the damage is already done. Goods can be bought and sold remotely without any personal contact between the buyer and the seller, allowing for an identity thief to intervene. The new electronic marketplace has emerged as the key venue for this crime as thieves have become cleverer and more tech savvy, deploying modern techniques and mechanisms to steal identities. Such techniques include skimming², data breaches³, phishing⁴, pre-texting⁵ and infecting computers⁶. According to the Consumer Report State of the Net Survey 2008, phishing alone has accounted for an estimated \$483 million total in damages in 2008. An estimated 1 in 13 households have provided phishers personal information last year, and 1 in 7 scam victims lost money. Mr. Hassan Abou Zeid, Chief Information Officer, HSBC Bank in Egypt confirmed the gravity and ease of phishing, stating that at HSBC, three phishing attacks have occurred so far this year. Such attacks are launched through fraudulent emails sent out to a million people, out those million, 30,000 will be HSBC customers and of those customers, 6 will reply by providing their personal bank details; becoming victims of fraudulent practices.

Therefore, as the development of technology has brought new, efficient ways to obtain more information; it has also brought severe drawbacks. Technology has heightened the impact of identity theft crimes since the stolen data can be rapidly distributed anywhere worldwide. As more people have access to technology, it has become difficult to control who is viewing information and to know where the information is located since it may be found in multiple sites. Despite the benefits of technological advancements, individuals are more susceptible to fraud.

² Skimming - a technique that is used to copy with a card reader electronically transmitted data on the magnetic strip of a credit card/ATM to enable the thief to make purchases. The skimmed information can then be transmitted via email anywhere in the world within hours after it is skimmed and commonly occurs in restaurants, hotels, gas stations and at ATM machines.

³ Data Breaches - penetration of a large data network by identity thieves targeting a vulnerable system, an unsecured network, or essentially any weak link. Once inside, the intruder is free to search and steal data, as well as move further inside the network to reach headquarters. Sometimes, the breached data is sold on websites.

⁴ Phishing - the process of sending out authentic-looking but fraudulent email designed to trick the respondent into giving out sensitive personal information.

⁵ Pre-texting - thieves call or text and claim to be from a bank or other organization requesting specific details. It is a practice similar to phishing.

⁶ Infected computers - thieves can employ a technique allowing internet users to infect themselves on their personal or work computers by falling for scam email or sharing their files with other users; in which usually the thieves' goal is to get a user with a vulnerable system to click a link.

Most businesses and websites lack a fully secure authentication mechanism to detect attempted identity theft. As long as this is the case, thieves will continue to find loopholes in the system and commit such crimes. For example, Europe adopted a Chip & Pin credit/debit card system that was quite efficient in authenticating individuals. However, within no time, thieves succeeded in bypassing this system, resulting in fraudulent transactions. Unless businesses and websites engage in a multi-layered authentication process that contains 'shared secrets,' fraudulent activities will persist. In other words, companies should request information from the consumer that only they would know, such as a relatively old phone number. However, at the same time, businesses and websites also need to prove their authenticity to the consumers to ensure them that their personal data will be protected.

II.2.a Increased mistrust at the user's level

As said, identity theft can harm the individual in a number of ways and is usually only detected well after the commission of the crime. Identity theft can result in some direct financial losses, damage to financial status and reputation, a possible civil judgment or criminal record, take time and cost to repair the damage, and cause emotional harm. Depending on the crime committed, the impact on the victim ranges quite broadly. Identity theft crimes that result from concealment or an identity thief opening a new account in the victim's name is more serious and harmful to the victim than unauthorized use of the victim's credit card, since it becomes more complex to prove the victim's innocence.

With regard to financial losses, upon realization and reporting of the crime, individuals in the United States are, according to Ms. Crane, protected under the consumer protection law from being liable for the amount the identity thief has stolen. Usually, they are liable for up to \$50 charged on their credit/debit card or ATM card. Restoring financial status and reputation, however, could be more complicated. It is an extremely time-consuming and nerve-racking process that oftentimes results in emotional harm. Sometimes the individual is not only a victim of an identity crime, but also victim to a false criminal record in instances where the imposter is charged and provides documents with his picture and the victim's information, including the victim's name and address. Thus, the victim might be issued a warrant in their name and possibly end up with a criminal record or inappropriate civil judgment. Furthermore, the 'bad' information disseminated by the thief then tarnishes the individual's profile as it reaches multiple locations through the electronic marketplace.

As a result, identity theft threatens consumer confidence in the electronic marketplace. Ms. Crane highlighted that in the US, according to the Wall Street Journal / Harris Interactive Survey, fears concerning the theft of personal information led 30% of consumers to limit their online purchases, while 24% were cutting back on online banking transactions. Such behavior ultimately impacts the economy; harming the electronic marketplace and disrupting e-commerce.

II.2.b Damage to the business

As already seen identity thefts are easier to commit than to track. Their impact on business and the economy is no smaller than that of consumer and brand fraud. As industries and businesses increasingly depend on the electronic marketplace to access information online, identity thefts thrive and prosper. It is thus imperative to be at least one step ahead in order to safeguard information, databases and transactions. Trust in the fairness and precision of the credit marketplace and the efficient regulation of this system depends upon such vigilance.

II.3 What has Microsoft Egypt done to address Identity Theft?

Mr. Karim Ramadan, General Manager, Microsoft Egypt, provided insight into the improved security features and activities undertaken by Microsoft worldwide in order to minimize fraudulent crimes and identity theft in particular. These global practices are then brought into the Egyptian market to protect the national consumers. He stated that Microsoft has incorporated phishing filters within Internet Explorer, integrated different spy ware detection products, as well as windows defender. In addition, Microsoft monitors and measures the amount of vulnerabilities or attacks that occur on their operating systems in order to find the weaknesses and loopholes and continue to improve their systems. As a result, due to increased security measures, Windows Vista has measured 45% less attacks than the previous operating system of Windows XP. Currently, Microsoft is working on a new and improved operating system that should be released soon. This system will protect against even greater threats.

III. Recommendations

As we have seen, deception and unfairness are two concepts indicative of the fraudulent practices of brand and consumer fraud as well as identity theft. Such practices have proven very detrimental to both the market and the individual. Thus, in order to mitigate the risks associated with identity theft, consumer and brand fraud, it is important to raise awareness for individuals, businesses and the government, and for all to react by undertaking certain actions and preventive measures.

III.1 Action by individuals

- Handle Personal Information with Care: Unfortunately, individuals tend to commit practices that put themselves at risk, such as carelessly disposing of important documents, mail, or bank statements. Such carelessness provides counterfeiters access to sufficient personal information to commit crimes of identity theft. Individuals should always shred important documents before disposal and regularly monitor accounts and financial statements.
- Employ common sense and analyze all irresistible offers: 'Extraordinary claims', 'no risk guaranteed' claims and 'quick and easy' claims should always raise a red flag.
- Utilize extra caution on the computer and internet: A valid anti-virus should be installed on all personal computers, which will detect destructive attacks by hackers, trojans, and malware/spyware. Individuals should also have difficult passwords in all

online accounts, and look for certifications for websites that indicate they are official. Additionally, greater awareness needs to be directed towards social networking websites, such as 'Facebook', where many people provide an abundance of personal information.

III.2 Action by businesses

- Like individuals, businesses must protect and manage all their data with caution.
- Properly identify customers and establish authentication programs: Banks must acquire all necessary information to certify an individual opening an account. They must ensure that they are the correct individual, identify the authentication of their customers, get to know the reasons behind opening accounts, etc.
- Invest in technologies and equipments to prevent and detect fraudulent activities: Technologies interfering with skimming devices should be installed on ATMs to protect from skimming. ATMs should also be equipped with cameras, so if someone does attempt to install a skimming device, their image will be captured.
- Detect suspicious behavior through monitoring: Pattern detection is another mechanism that businesses should invest in, which is a system that would detect suspicious patterns. For example, the purchases undertaken on a stolen credit card would differ from the normal pattern of the card-owner. By detecting specific patterns, a bank can identify malicious behavior and attempt to limit the damages.
- Monitor and examine customers' reactions to products/services and return rates: It is crucial that businesses regularly examine consumers' reactions to products and services and monitor their return rates in order to identify if there are fraudulent activities occurring with their products. Also, if there is a high level of complaints or a consistency in complaints, then it can be a cue to analyze the business practice and determine if there are deceptive, unfair, or counterfeit practices occurring.
- Employ best business practices: Such as the disclosure of material information, the substantiation of claims, due diligence in knowing clientele, and monitoring clients⁷.
- Engage in self-regulation to help remedy injury to consumers: Businesses should alter advertisements and claims upon realization of a problem. They should also improve training, monitoring, and disciplining of their sales staff as well as firing staff that has been utilizing deception to sell products.

III.3 Action by government

- Investigate Businesses: Governments have the ability to contact the target or the business with a deceptive sales practice, interview consumer witnesses, request

⁷ Disclosing material information that would likely affect a person's choice of goods or services is important. All material information should be clearly and conspicuously disclosed to consumers, especially before the consumer pays for the goods or services. Material information can include information on cost and quantity of goods or services, as well as a refund policy, material restrictions, limitations and conditions. Substantiation should exist before an advertisement or representation is displayed publicly, and should be able to support all the objective claims in the advertisements. Due diligence and monitoring of clients go hand-in-hand as they apply to businesses whose clients are other businesses. Therefore if a business monitors their clients and analyzes their clients well before committing to them, then the business helps to avoid consumer harm by being selective about each business that they are interacting with.

- information and documents from third parties, review public records – such as court filings or corporate records, and conduct undercover telephone calls and purchases that can help review the product to determine if it can actually perform as promised.
- Request appropriate remedies: Such as consumer redress, restitution, civil penalties, rescission of contracts or collective advertising⁸.
 - Enforce anti-spam awareness campaigns: Spam is a very crucial tool and cross-border activity that is used by fraudsters worldwide. Although there is a Cyber Crime Unit established within the Egyptian government, in line with the Homeland Security in the United States, there are no current laws or mechanisms in place to combat spam in Egypt. Thus, such laws or mechanisms need to be established in order to avoid these types of cyber crimes.
 - Provide examples of fraud or deception to the community: The government has to depict scenarios of fraudulent cases to the public in order to educate consumers and show the perpetrators the penalties they can encounter.
 - Improve enforcement of IPR protection: Among the real challenges encountered in Egypt are the enforcement and implementation of the established legal framework for IPR. The government needs to focus on enforcing strong IPR protection to reduce the impact of the counterfeit economy. It is incumbent upon the government to establish a solid base of well-trained custom officers fully cognizant of their responsibilities in preventing and undercutting any attempts to import pirated and counterfeited goods.
 - Link the activities of various ministries with the CPA: Even though there is existent cooperation in Egypt between different ministries and the CPA to counter the widespread and harmful practices of illicit trade and fraudulent crimes, additional effort is still required. A clear example of a successful co-operation has been the agreement between the CPA and the Ministry of Education to integrate consumer protection and internet safety topics in curriculums of different education levels starting in 2010 and 2011.

Conclusion

With the ever expanding and deepening globalization of the world economy and the unprecedented development of novel information technology, digital infringement and fraud has proliferated. It is important that immediate action is taken in order to mitigate harm to consumers, businesses, the economy and the society as a whole. Upon assessing identity theft, consumer and brand fraud, it is imperative to stress the need for joint efforts amongst the different stakeholders to counter these crimes. This is not a problem that one entity can address alone. The interdependence between the different stakeholders –each experiencing the repercussions of crimes in the new economy in their own way–

⁸ Consumer redress - a monetary remedy to reimburse the consumer for the stolen amount.

Restitution - puts the consumer in the position they were in before deception as well as including additional costs such as bank fees that may have been incurred as a result of the fraud.

Civil penalties - provide for penalties that may be much higher than the consumer redress amount.

Rescission of contracts - voids the contracts between the consumer and the business so that the business cannot collect or sell the contract.

Collective advertising - halts the business from making a deceptive representation in advertisements, as well as telling consumers that the representation was not true.

necessitate continued collaborative thinking to generate new ways and means to fight the crimes of this millennium. Minister Rachid, in his keynote speech, could not stress enough this need for 'further joint efforts and aligned activities amongst consumers, the government, and non-governmental organizations in order to prevent identity theft and consumer and brand fraud, which are crimes that thrive in an open and free economy.'

This kind of collaboration must be complimented by increased efforts towards awareness-raising. It is vital that further efforts are made to protect consumer choice, help individuals fight deception, and inform and educate all the key players so that confidence in the free markets is strengthened. Awareness should also go hand-in-hand with incentives. Once individuals know the detriments of fraudulent and counterfeited goods, alternatives and encouragement to entice consumers not to buy these goods will be necessary as consumer demand remains a key factor in the popularity and success of widespread fraud. All the stakeholders hold equal interest in overcoming these challenges and with cooperation and the dissemination of information, the Egyptian economy can be protected from the proliferation of these grave breaches.