**Identity theft- the investigation, implication and alleviation on the Jamaican society.**

**Group Members:**

Ronique Dixon-0603936

Ruth Meredith-0904441

Shauntae Mitchell-0903758

Kareem Scott-0900067

The University of Technology, Jamaica.

School of Computing and Information Technology.

**Introduction**

"Identity theft does not discriminate. It is happening to the rich and the powerful. It is happening to the average person on the street “(Gertler, 2011).

According to the authors in Perspectives on Identity Theft, identity theft can be refered to as an instance in which an individual’s personal information is used by another to facilitate an act of fraud. The term identity theft, which did not appear until the late 1980s, was initially used to distinguish individual victims (identity theft) from collective victims (identity fraud) – both of whom were harmed by the same set of criminal activities (McNally and Newman, 2008). The US Identity Theft and Assumption Deterrence Act (1998) states that identity theft occurs when a person “knowingly transfers or uses, without lawful authority, of a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable state or local law”.

The incidence of identity-related crime has increased considerably since the advent of computers and Internet owing to the ability of digital technologies to facilitate the fabrication and alteration of documents used to establish identity, and to enable personal information to be located with ease from electronic databases (Smith, 2008).

This literature review explores the body of knowledge related to identity theft as well as different ways in which it is being done. It attempts to demonstrate the practicality of fully exploiting the use of Biometric Data in attempting to minimize identity theft, highlighting the long-term benefits of implementing this type of system.

**Identity Theft**

A poll conducted by Ipsos-Reid (2006) found that 4% of Canadians have been subject to identity theft and 20% know someone who has been affected. Studies have shown that criminals may gravitate towards identity theft because the risk of getting caught is not very high. According to CIPPIC (2007), identity theft has become a crime of choice for criminals because of “the possibility of a very high return combined with a very low risk of getting caught. Few individuals are ever charged with and convicted of identity – theft related crimes”. Access to personal information of individuals is readily available from a variety of sources. “Hospitals, governments, cell phone providers, credit card companies and other corporate entities regularly collect and store this information, sometimes without the knowledge and consent of the individuals concerned and not always with appropriate safeguards”. Advancement in technology has also facilitated the ability of thieves to steal personal information. CIPPIC (2007) also noted that the use of copying equipment, computers, and the Internet and data warehouses is used to acquire information.

**Identity Theft in Jamaica**

Researcher Helps (2012) pointed out that Identity theft is a big deal not because of loss of money but it is because of the implications that it has on an individual. It is taking over someone persona. “Falsifying Taxpayer Registration Numbers (TRNs) is the fastest growing form of identity theft”, (Helps, 2012).There has been an increase in the number of identity theft in Jamaica which is driven by deportees without established identities and just wants to get something and move stated by superintendent Clifford Chambers to the Jamaica observer in 2012.

Researcher Tyrone Reid (2012) reported that The Department of Correctional Services uncovered what appears to be an elaborate identity-theft scheme involving fraudulent taxpayer registration numbers (TRN) and fake voters' identification cards in the name of employees. “Evidence revealed that staff members’ names and identities are being used to access loans without the individuals even knowing. It was observed that the applicants used Electoral Office of Jamaica issued ID cards with the same name of staff members but with a different photograph, the same TRN number but the photocopied TRN card that is on the application form is different from the card being held by the actual employee,” said Lieutenant Colonel Sean Prendergast (Reid 2012).

**Implementation of Anti-Identity Theft in Jamaica**

In an article published in the Jamaica Observer in October 2012, it stated that the Registrar General’s Department (RGD) has increased its efforts to combat an underground fraud network that the agency says is involved in widespread identity theft.They have created an Authentication, Verification and Identity Department (AVID), which conducts record updating and verifies supporting documents and vital records. RGD stated that perpetrators are stealing identities from both living and dead people. For the financial year of 2011, 150 copies of birth certificates were taken and confiscated from people. Most of these people were visa applicants. RGD's acting marketing and planning manager, Hazel Cunningham, stated that the agency will create a greater public awareness about identity theft by embarking on a number of community outreach programmes and they will also work along with the Passport, Immigration and Citizenship Agency and embassies.

**Impact of Identity Theft in terms of Monetary Costs in Jamaica**

In Jamaica, financial institutions are now being given direct access to the TRN database, and credit card fraud should become more difficult when plastic fitted with microchips are introduced locally next year (Thame 2012).Banks in Jamaica lose millions of dollars annually due to cloning of credit and debit cards.Wendell Smith, overseer of information technology at Jamaica National Building Society (JNBS) stated that presentation of TRNs at the bank to carry out transactions is a procedure that is done on a daily basis. When the number is presented, it would be checked to make sure it belongs to the person presenting it. This poses a lot of problems sometimes as people come in with falsified TRNs. The police have identified falsifying taxpayer registration numbers in Jamaica as the fastest-growing form of identity theft.

Smith also stated that a consortium inclusive of Mastercard and Visa is going to make credit cards with chips compulsory in the Latin America and the Caribbean in 2013(Thame 2012). All financial institutions will have to change out the existing cards and replace them with the chip cards. As a result, it will be more difficult for the cards to be cloned which will reduce the illegal use of credit cards.

**Identity Theft in Other Countries**

# The phenomena of identity theft have also affected several other islands in the Caribbean. According to the article entitled “Electronic card fraud and identity theft in the Caribbean” there is a debit card and identity theft beginning to spread over several parts of Bridgetown Barbados (Gill, 2012). According to Jeff Gill (2012) accounts of 17 persons have had their moneys illegally withdrawn from several automatic teller machines. This type of identity theft was referred to as skimming where thieves use a device to steal credit card information. “The card is run through what is called a skimmer which harnesses the name of card holder, account number expiration date, verification/CVV code, and even the PIN number”.

# In 2004 the Internal Revenue Service has seen signs of a fraudulent scheme targeting non-resident who have income from a United Sates source spreading in the Caribbean. This phenomenon has surfaced in the Caribbean countries such as Barbados, Puerto Rico, Trinidad& Tobago, and the Turks & Caicos Islands. “The scheme uses fictitious IRS correspondence and an altered IRS form in an attempt to trick the foreign individuals into disclosing their personal and financial data. The information fraudulently obtained is then used to steal the taxpayer’s identity and financial assets” (anonymous, 2004).This practice is referred to as phishing.

# According to the article entitled “ID Theft Growing Rapidly in 2009” by Richard Adhikari, identity theft is America's fastest-growing crime. The figure for this crime is going at an alarming rate. “ Report from the Identity Theft Resource Center (ITRC), a nonprofit set up to support and educate consumers on identity theft, U.S. businesses and other organizations suffered 83 security breaches so far in 2009 -- potentially exposing the records of at least 1.1 million people.”  Richard Adhikari (2009) further went on to report that updated findings illustrated that the pace of data breaches is increasing. “Breaches struck 656 businesses, government agencies and other organizations last year, an increase of 47 percent over 2007.” According to the article “Identity theft growing 10 percent per year, experts warn” identity theft is growing at a rate of 10 per cent a year and one in four adults in the united State will become victims as well one in 20 adults ( Sparacello, 2010).

# According to the article entitled “Largest Identity Theft Case In U.S. History: Amar Singh And Wife, NehaPunjani-Singh, Plead Guilty To Massive Fraud”, ,Amar Singh And Wife, NehaPunjani-Singh, pulls of the largest identity theft case in US history (Compton, 2012). “They would receive information about unknown people from various foreign countries, such as Russia and China, as well as via statewide suppliers — who would use a skimming device to swipe consumer credit card information at retail or food establishments — and illegal identification-gathering websites”. Singh would employ personnel to shop around the U.S with the counterfeit credit card and I.D cards manufactured using the stolen information.

With identity theft still on the rise and increased measures to combat them, there are yet numerous evidences of identity theft cases still emerging. In a book titled Perspectives on Identity Theft the authors spoke about surveys done by the National Crime Victimization Survey which reveals that in the United States of America Nineteen (19%) percent of the survey sample resided in California, nine (9%) percent in Florida and five (5%) percent in New York, which ranked among the top seven states in America being affected. (McNally and Newman 2008) The survey went on further to note that financial ID was the highest method engaged in followed by criminal ID theft and to a lesser extent cloning. Cloning is where a criminal acquires personal identifiers and then impersonates someone else in order to conceal his or her true identity from authorities. (McNally and Newman 2008) In another survey done by Synovate (2003), it also revealed that “Hispanics and African Americans were twice as likely as Asians and Whites to experience the most serious type of fraud, and also that middle-aged persons tend to become the victims of larger dollar amount frauds.”

In a report done by CBS News in February 2009 gives an overview of a prominent case of identity theft. This is the story of a restaurant busboy in America who stole millions of dollars from celebrities through the use of the Internet and Forbes Magazine’s list of the richest people in America. The perpetrator, Abraham Abdallah decided to target well-known figures such as Oprah Winfrey, Martha Stewart and Steven Spielberg. He is a high school dropout, who has now been charged with criminal impersonation, forgery and fraud. The report gave a synopsis of how Abdullah carried out some of his acts; he would use computers at a library, Web-enabled cell phones, virtual voicemail and hired couriers, to obtained social security numbers, credit card numbers and all vital financial records.

His recent schemes lasted for about six months and requested the services of couriers and even prostitutes to deliver expensive items bought with the victims’ credit cards. He was later discovered through suspicions when he sent an email requesting a large sum of money to Merrill Lynch to send cash to an account to that of Thomas Siebel of Siebel Systems. These kinds of acts are nothing new for Abraham Abdullah as he has had similar offenses in the past for bank fraud from an early age of 18; some of shenanigans were even done outside of the US.

One might ask where does this leaves victims or what effect does this have on them? A recent research points out that there are many reasons to believe that fraud victims suffer just as many, if not more negative experiences than victims of common crime. During a savings and loan crisis in the 1980’s, it was reported that the victims of identity theft (mainly retirees) were extremely distraught leading to a few committing suicide while others developed psychological problems.

**Jamaica Cyber Crime ACT 2010 to help prevent Identity Theft**

1. In this Act ----

* “Damage” for the purposes of section 3(3), 5(3), 6(5), 7(2) and 8(2), means any impairment to a computer, or to the integrity or availability of data that---

1. Causes economic loss;
2. For the purposes of this Act, a person obtain access to any program or data held in a computer if he causes a computer to perform any function that ----
3. Copies or moves the program or data to any storage medium other than that in which the program or data is held or to a different location in the storage medium in which the program or data is held.
4. For the purpose of this Act, a person who accesses, modifies, or uses, any program or data held in a computer, or causes the computer to perform any function, does so without authorization if ---
5. He is not himself entitled to control the access, modification use or function of the kind in question;
6. He does not have consent for the access, modification, use or function of the kind in question from any person who is so entitled;
7. A person who knowingly obtains, for himself or another person, any unauthorized access to any program or data held in a computer commits an offence

**Impact of Identity Theft in terms of Monetary Costs in America**

# The Internal Revenue Service (IRS) may have lost billions to identity theft. According to Josh Lederman (2012), the IRSmay have delivered more than $5 billion in refund checks to identity thieves who filed fraudulent tax returns for 2011. They estimate another $21 billion could make its way to ID thieves' pockets over the next five years. The IRS detected about 940,000 fraudulent returns for 2011 claiming $6.5 billion in refunds, there were potentially another 1.5 million undetected cases of thieves seeking refunds after assuming the identity of a dead person, child or someone else who normally wouldn't file a tax return.

**Systems to Handle Identity Theft in Other Countries**

In Honduras, the National Registry of Persons (RNP), which is in charge of providing identification cards, wants to make it more difficult for criminals to commit identity theft in their nation.The RNP expects to introduce an ID card printed on high-quality laminate containing a microchip that will store the owner’s marital status, social security number, driver’s license, taxpayer number and general medical information(Novoa 2012). They want to introduce a new system because it is rather easy for criminals to create forged documents and so by using high-quality laminate with the chip, the material used will be hard to forge.

In the UK, the General Register Office for England & Wales and its Scottish and Northern Irish counterparts sent encrypted files containing details of everyone who has died in the UK each week to vetted organizations, including credit-checking agencies. The move was intended to prevent criminals using the identities of the dead to open bank accounts, commit benefit fraud or aid illegal immigration (Anonymous 2008). The announcement happened simultaneously with the start of National Identity Fraud Prevention week (a government-backed awareness drive to warn of the risks of ID fraud).

**Biometric Solution**

“Biometry is a statistical analysis of patterns obtained by compiling readings of physiological characteristics or behavioural characteristics for positively identifying a living person.” (SANS Institute, 2002).According to Gemalto, a company that provides electronic identity solutions, biometrics has quickly established itself as the most pertinent technology for identifying individuals in a fast and reliable way through the use of unique biological characteristics (Gemalto, 2012). Many programs now-a-days are relying on biometrics and these programs that are used for the general public are now seeing rapid development. These programs are being predominantly introduced by national authorities, as the overall management of population’s fingerprints call for tightly regulated legal and technical framework (Gemalto, 2012).

An application/program that has been deployed on a wide scale is the electronic passport. It stores two fingerprints along with the passport photo. Another application that exists mainly in European and Middle East countries is the “national identity cards”. In this application, fingerprints are used to confirm the card holder’s identity before he or she is given access to whatever services are needed.

Vivian Chu (2009) conducted a study among individuals of varying backgrounds and ages to help determine their views on biometric technology. The study revealed that “77% of respondents thought that biometric technologies are a useful tool for authentication of identities…Only 7% were opposed to using biometrics. The technology that respondents most widely accepted was fingerprint recognition”. Chu’s study also revealed that enhanced security was thought to be the greatest benefit of biometric technologies.

In a paper entitled Biometric Technology Stomps Identity Theft, the writer highlighted some of the benefits of implementing Biometric Technology Products (BTP). The reasons for using BTPs include the positive authentication and verification of a person, ensuring the confidentiality of information in storage confidentiality of information in storage or in transit. Other reasons are the non-repudiation of acts or transactions, deterrent of identity theft, convenient, safe, non-intrusive, and reduced administration costs compared to passwords. The effectiveness of BTPs is increased if biometric solutions are implemented in combination with Smart Cards and PKI (Public Key Infrastructure) (Zegiorgis,2012). BTPs help to uphold the protection of information in databases including customers and teller identification using fingerprints, iris and facial recognition, ATM access using iris and facial recognition, transactions in transit over the telephone suing voice recognition, computer-aided online transactions using voice, iris, fingerprint and facial recognition and point of sale (POS) transactions using dynamics and fingerprint (Zegiorgis,2012).

According to CIPPIC (2007), there are various methods that can be used to steal personal information. Some of these methods are “relatively simple and low tech (such as: reading obituaries; stealing mail from homes, businesses and mailboxes; breaking into offices or vehicles to steal files; stealing luggage and briefcases; and rummaging through home and businesses’ garbage)”. Other methods that are more sophisticated will include “stealing or hacking into computers; impersonating clients when calling insurers, credit card companies; using the services of online information brokers; and duplicating magnetic strips on the back of cards. These methods can be exercised either in person or virtually through the internet, phone lines or cell phones.”

Sara Berg from the School of Criminal Justice, University of Albany explores the various techniques used in each form of identity theft. For non-technology related offenses, stealing the victims purse of wallet may provide access to a great deal of data; mail theft , where documents such as pre-approved credit card applications are stolen directly from a mailbox; within an organization , dishonest employees with access to sensitive data can obtain Social security number and other records. On the other hand she went on further to discussed how technology(IT) based offenses occur where personal and credit information can be taken from unsecured online shopping sites; using “pretexting, a method for obtaining personal information under false pretenses mission, an offender could pose as a telemarketer or a financial representative to lure victims in disclosing sensitive information.

**References**

# Anonymous.(2004). ID Theft Growing Rapidly in 2009.*RS REISSUES CONSUMER*

# *WARNING ON IDENTITY THEFT SCHEME; SCHEME NOW TARGETING CARIBBEAN*.Retrieved November 3, 2012 from http://www.quatloos.com/caribbean\_ID\_theft.htm

# HELPS.H.G (2012, May 21). Identity theft growing.*Jamaica Observer.*

Anonymous (2012, October 03). RGD sets up unit to curb identity theft. *Jamaica Observer.*

CIPPIC. (2007, March). *Identity Theft: Introduction and Background*, CIPPIC Working Paper

No.1 (ID Theft Series), Ottawa: Canadian Internet Policy and Public Interest Clinic.

Newman, R., M. M. (2008). *Perspectives on Identity Theft.*

Thame, C. (2012, September 8). Clampdown on identity theft.*Jamaica Observer.*

Jederman, J (2012, August 02). IRS May Have Lost Billions To Identity Theft. *HuffingtonPost*

Novoa, R (2012, June 08) Honduras: Identity Theft Concerns Authority. Retrieved from

http://infosurhoy.com/cocoon/saii/xhtml/en\_GB/features/saii/features/main/2012/08/06/f eature-01

### Adhikari, R. (2009). Caribbean Identity Theft Scheme.*The figures for ID theft are growing at an*

### *alarming rate*.Retrieved November 3, 2012 from http://www.esecurityplanet.com/news/article.php/3808196/ID-Theft-Growing-Rapidly-in-2009.htm

CBS. (2009, February 11). *Cybertheft Case Skewers Celebs.* Retrieved October 31, 2012, from http://www.cbsnews.com/2100-500164\_162-280107.html

Chu, V. (2009).*Use of Biometrics,* TechCast Article Series. Retrieved from [http://www.techcast.org/Upload/PDFs/634122830612738824\_Biometrics- VivianandGayathrilo- res.pdf](http://www.techcast.org/Upload/PDFs/634122830612738824_Biometrics-%09VivianandGayathrilo-%09res.pdf)

# Compton, A. (2012). *Largest Identity Theft Case In U.S. History: Amar Singh And Wife, Neha*

# *Punjani-Singh, Plead Guilty To Massive Fraud.*Retrieved November 3,

Erin, R. (2009, September 5). *Catch Him If You Can.* Retrieved October 30, 2012, from http://listverse.com/2009/09/05/10-bizarre-cases-of-identity-theft/

Gemalto (2012).*Biometrics for use in identification.*Retrieved November 5, 2012 from https://www.gemalto.com/biometrics/index.html

# Gill, J. (2012).*Electronic card fraud and identity theft in the Caribbean.*Retrieved November 3,

Ipsos-Reid (2006, March 7). *One-Quarter of Canadian Adults (24%) Have Been Touched by Identity Theft*. Retrieved October 2012 from [http://www.ipsos-na.com/news- polls/pressrelease.aspx?id=2998](http://www.ipsos-na.com/news-%09polls/pressrelease.aspx?id=2998)

Reid, T. (2012, July).Identity theft Hits Prison Service.*The Jamaica Gleaner.*Retrieved

November 3, 2012 from htt://www. jamaica-gleaner.com.

SANS Institute (2002).*Biometric Technology Stomps Identity Theft*. Retrieved October 2012 from [http://www.sans.org/reading\_room/whitepapers/authentication/biometric- technology-stomps-identity-theft\_126](http://www.sans.org/reading_room/whitepapers/authentication/biometric-%09technology-stomps-identity-theft_126)

# Anonymous (2008, October 5). *Registrars' death lists 'will fight ID fraud' and identity theft* Retrieved from http://www.telegraph.co.uk/news/uknews/law-and-order/3142021/Registrars-death-lists-will-fight-ID-fraud-and-identity-theft.html

# United States. House of Representatives (1998, October 30). US Identity Theft and Assumption Deterrence Act. Washington DC.

CIPPIC (2007), "Techniques of Identity Theft", CIPPIC Working Paper No.2 (ID Theft

Series), March 2007, Ottawa: Canadian Internet Policy and Public Interest Clinic.

Crime Prevention Studies, volume 23 (2008), pp.151-167.