

**ALBERTA
INFORMATION AND PRIVACY COMMISSIONER**

**Report of an Investigation into the
Security of Personal Information**

September 26, 2006

MD Management Ltd.

Investigation Report P2006-IR-005

I. INTRODUCTION

[1] On June 30, 2006, the Information and Privacy Commissioner (“the Commissioner”) was notified by MD Management Ltd. (“the Organization”) that one of its laptops containing its clients’ personal information was stolen. The Organization outlined the various measures it had taken to mitigate risks of harm to the affected individuals. The Commissioner elected to conduct an investigation to determine whether the incident represented a contravention of the *Personal Information Protection Act* (“PIPA” or “the Act”).

II. JURISDICTION

[2] PIPA applies to provincially-regulated private sector organizations operating in Alberta, including MD Management Ltd. PIPA sets out the provisions under which organizations may collect, use, or disclose personal information, and also places a duty on organizations to protect personal information in their custody or control against such risks as unauthorized access, collection, use, disclosure or destruction.

[3] The Commissioner has jurisdiction in this case because MD Management Ltd. is an organization, as defined in section 1(i) of the Act. The personal information in question was housed in the Organization’s Alberta branch.

[4] Section 36 of the Act empowers this Office to conduct investigations to ensure compliance with any provision of PIPA and make recommendations to organizations regarding their obligations. The Commissioner decided to initiate an investigation of his own accord. Pursuant to section 49 of PIPA, the Commissioner authorized me to investigate this matter. This report outlines my findings and recommendations, which may be made public according to section 38(6) of the Act.

III. STATEMENT OF FACTS

[5] CMA Holdings Inc. is the holding company for the Canadian Medical Association, a national public health and physician advocacy group. CMA Holdings oversees various companies including its distinct subsidiary, MD Management Ltd. (the organization involved in this incident). MD Management offers financial products and services to Canadian Medical Association members and their families. These services are offered in 47 branches across Canada, including Edmonton, Alberta.

[6] On May 30, 2006, a senior employee of MD Management in Edmonton copied a spreadsheet file onto his company laptop in order to review the client list of the financial consultants reporting to him. The laptop was not in a typical laptop case; instead it was carried in a soft briefcase-style bag. The laptop had a sticker on it stating "Property of MD Management" with a bar code and computer ID number.

[7] On June 19, 2006, while en route from one MD Management office to another, the employee made a stop at a store and parked his vehicle. He locked the vehicle and left the laptop inside. When he returned 10 minutes later, he noticed that someone had gained entry to his jeep by unzipping the back passenger-side window of the soft top. The bag containing the laptop was missing in addition to various other personal items in the vehicle. The employee immediately notified his employer and police of the theft.

[8] Shortly after the incident, MD Management contracted a firm to conduct a private investigation to try to retrieve the laptop, as well as to assist with MD Management's own data security review. The Organization determined that the spreadsheet file contained personal information of approximately 8,000 individuals, most of them Albertans. The records for the individuals consisted of:

- name
- age, month and year of birth (no *day* of birth)
- medical specialty
- home address and phone and fax numbers
- business address, phone and fax numbers
- home and/or business email address
- total financial assets with MD Management (in some cases)
- shareholder number (in some cases)

[9] The shareholder number is not an account number for specific investments. Rather, it is an identifier for each individual client who may have several investment accounts. The file did not contain Social Insurance Numbers (SIN), *day* of birth, investment account numbers, credit card numbers or banking information. It should be noted that PIPA does not apply to business contact information, as described in section 4(3)(d) of the Act, when used to contact individuals in their business capacity. In the present case, the business

contact information is considered personal information because the Organization would be contacting these individuals as consumers of its products and services and not in their business capacity as physicians.

[10] The laptop's operating system (Windows 2000) had a standard log-on password requirement. The password was an alpha-numeric string that no one other than the employee and authorized managers within the Organization's IT department knew. The file containing the personal information was neither password-protected nor encrypted.

[11] The remote access feature for connecting the laptop to MD Management's network required an alpha-numeric username and password. There was no auto-fill-in feature for these fields. Immediately following the theft, MD Management disabled this username and password. After five failed attempts to gain remote access, MD Management's system prohibits further attempts for 24 hours. To date, the Organization reports that no attempts have been made to gain remote access to its network from the stolen laptop. There have not been any reports of malicious use of the personal information contained on the laptop either. At the time of writing this report, the laptop had not been recovered.

IV. ISSUES

[12] The issue to be examined in this report is:

Did the Organization make reasonable security arrangements to protect the personal information in its custody, in accordance with section 34 of PIPA?

V. ANALYSIS

Did the Organization make reasonable security arrangements to protect the personal information in its custody, in accordance with section 34 of PIPA?

[13] Section 34 of PIPA establishes the following duty:

An organization must protect personal information that is in its custody or under its control by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure, copying, modification, disposal or destruction.

[14] MD Management's duty to safeguard personal information is indisputable. The matter to be examined is whether the Organization's protection measures constituted "reasonable security arrangements" against the risks outlined. If not, the organization was not in compliance with the Act

and a breach of the duty to safeguard personal information occurred. Thus, for a breach to occur, actual unauthorized access or real incidents of misuse need not have occurred. The Act requires an organization to guard against reasonably foreseeable risks. Generally, it is not necessary that safeguards be flawless in order to be deemed reasonable. An organization need only demonstrate that it implemented deliberate, prudent and functional measures that displayed consideration toward risk mitigation in order to be in compliance with the Act.

MD Management's Safeguards

[15] The safeguards to be evaluated in this matter are described in MD Management's *Corporate Information Security Policy*. According to it, the Organization has permission controls in place to ensure that only authorized employees can access personal information needed to perform their duties. With respect to laptop security, the policy states a laptop:

- must always be safeguarded from theft
- must never be left unattended
- must be locked in secure cabinets when leaving the office even if the laptop can be secured to the workstation
- must be carried on the plane when traveling
- must never be left unattended in a car or hotel room etc.

[16] According to the policy, violations of these requirements could result in disciplinary action. This laptop portion of the policy is augmented by the MD Management guidelines, "Travelling with a Laptop". This document gives employees advice which includes:

- don't keep data on the laptop unless you need to
- laptops are an obvious target for theft
- never leave your laptop unattended
- if you set your laptop down for any reason keep a close eye on it or put it in a place where you can feel if someone grabs it
- ALWAYS keep your laptop within your sight lines

[17] These guidelines outline situations and scenarios in which laptops are vulnerable, such as in washrooms and at check-in counters. It advises employees to hook the case strap around their feet or hands so that its movement can be easily felt when attention is diverted from it. The policy is detailed and gives sound advice.

[18] In addition to relying on employee compliance with the policy, MD Management has a technical defense measure in place: the laptop system's log-on password. MD Management's policy requires that laptops be pre-configured by its information technology (IT) department. Part of this configuration includes log-on password protection and a screen saver password protection. These features were engaged on the stolen laptop. The policy also requires that users password protect files containing personal information. Although the

Organization's laptops were equipped with a system designed by MD Management to encrypt information downloaded onto a specific portion of the hard disk, this was not expressed in company policy. Unfortunately, the file in question was not stored on this protected portion of the laptop.

[19] MD Management determined that the employee in this matter violated corporate policy by leaving the laptop in his vehicle, by storing more personal information on it than he required (i.e. more data fields than essential), for longer than was necessary, and by failing to password-protect the file.

[20] In section 2, PIPA defines the standard as to what is reasonable as "what a reasonable person would consider appropriate in the circumstances". No other guidance is offered.

[21] To determine whether MD Management took "reasonable" security precautions, I will examine: whether the security risk was foreseeable and the likelihood of damage occurring; the seriousness of the harm; the cost of preventative measures, and relevant standards of practice. These factors have been useful in determining negligence in civil law cases and I am of the view that they have relevance here.

Foreseeability of Security Risk & Likelihood of Damage

[22] The risk associated with leaving valuables inside a vehicle is well known. Signs in parking lots warning motorists not to leave valuables inside their vehicles are commonplace. The Insurance Bureau of Canada advises among its top ten precautions to "Never leave valuable objects or packages in full view. Put them in the trunk."¹ The Calgary Police Service's website reminds citizens to: "Hide Your Valuables - Don't leave valuables in your car. If you must, then store them in the trunk, out of sight"².

[23] Normal human behaviour often operates in disregard to warnings and well known risks. In a victimization study published by the Canadian Research Institute of Law and the Family, it was found that 19% of Albertans had been victimized by theft from their vehicle in the previous three years³. According to Edmonton Police, in the first quarter of 2006 alone, there were 1,241 reported thefts from vehicles in the City of Edmonton⁴.

[24] Acknowledging this issue, MD Management has a policy in place prohibiting employees from leaving laptops unattended. The policy, an important and necessary step, is required to be read by every employee and states that there are consequences for violation. In the present case, the employee violated corporate policy by, among other things, leaving his laptop unattended in his car. MD Management states that responsibility to protect personal information is up to the employee:

¹ Insurance Bureau of Canada. "Automobile theft: It's costing everyone too much"

² <http://www.calgarypolice.ca/crimeprev/frame1.html>

³ Canadian Research Institute for Law and the Family. *Perceptions and Experiences of victimization in Alberta: Findings from a Survey of Alberta Adults* [2002].

⁴ http://www.watch.edmonton.ab.ca/crime_stats.htm

It is the laptop user's responsibility to ensure that the confidential information and the corporate asset are safeguarded while in his/her possession at all times.

[25] Organizations are ultimately accountable under PIPA for the conduct of their employees. Similarly, under the *Personal Information Protection and Electronic Documents Act* ("PIPEDA"), the Privacy Commissioner of Canada found in Case Summary #289 that although an organization may have policies in place regarding laptop security, employees' lack of compliance still renders the organization accountable:

As for the safeguards, the Assistant Commissioner noted that, with respect to laptop computers, the bank had policies and procedures in place that required passwords and safe physical storage of the computers. Although these policies and procedures appeared to meet the requirements of Principle 4.7, the financial planner in this instance did not follow the bank's recommendations regarding physical security, and left the laptop unattended on the seat of her vehicle. The Assistant Commissioner therefore found the bank in contravention of Principle 4.7.

[26] The likelihood of employees failing to adhere to organizational policy and procedure was examined by Palisade Systems Inc., a network and data security company. In its survey of 127 companies who reported data breaches in the United States in the past year, 54% indicated that the breach was a result of "employee error"⁵. Thus, an important consideration in designing reasonable security arrangements is that humans are naturally fallible and any personal information safeguards must account for this. Employees may neglect to delete files they no longer need, fail to activate file password protections or leave laptops in cars, as was the case here.

[27] Theft of corporate laptops from employees has been well publicized. In the past year, the Privacy Commissioner of Ontario reported five known incidents in which corporate laptops containing personal information were stolen from employees' cars and homes. (HI-050044-1, HI-050039-1, HI-050026-1, HI-050022-1 and HI-050003-1). Last fall in Quebec, an employee of the National Bank of Canada had 700 customers' banking, credit card and SIN numbers stored on a laptop which was stolen from the employee's home.

[28] In May of 2006, the theft of a United States government laptop containing the personal information of over 26 million American Veterans was highly publicized. In June 2006, the U.S. Federal Trade Commission experienced two laptop thefts from an employee's vehicle exposing 110 individuals' personal information. Around the same time as the MD Management incident, in the United States, Armstrong World Industries experienced a laptop theft from an employee's vehicle disclosing the personal information of 12,000 other employees. The American Navy reported two missing laptops this year containing the personal information of 31,000 recruiters and prospective recruits. The American Transport Department recently made news when one of its laptops containing 133,000 pilots' personal information was stolen from an employee's vehicle. In one of two of Ernst & Young's laptop thefts this year, 243,000 Hotels.com customers' information was

⁵ <http://www.palisadesys.com/news/releases/view.php?pressreleaseid=80>

compromised. ING, Equifax, and Boeing also experienced laptop thefts over the last year causing serious security concerns for thousands of employees and customers. In the first half of 2006 alone, consumer advocacy group Privacy Rights Clearinghouse reports more than 20 other incidents in which laptops containing personal information of millions of individuals were lost or stolen directly from employees⁶.

[29] These recently publicized laptop thefts represent only a cursory list of reported incidents over the past three years. Still, it demonstrates that the theft of corporate laptops from employees has not been an unforeseen risk. Rather, laptop theft has been the subject of discussion in the media and experienced by numerous organizations, affecting the security of millions of North Americans' personal information. MD Management's own policy acknowledged this risk in detail by advising employees never to leave laptops unattended and explaining how laptops are stolen.

[30] It is likely that many of these organizations had similar policies in place prohibiting employees from storing unnecessary personal information on laptops and leaving laptops unattended. It is reasonable to conclude, therefore, that such policies and guidelines are insufficient. These cases make clear that organizations cannot have all confidence that employees will or can remember to adhere to these policies. Absolute supervision of a laptop is not possible, and is a fact that thieves count on. Leaving the security of laptops entirely to employees is not reasonable given that laptops can be stolen from their homes or even taken from them forcefully. Recent restrictions during air travel compel travelers to relinquish custody of laptops and check them in. An employee cannot be held accountable for the theft or loss of the laptop by an airline in such circumstances. Human nature and circumstances beyond the control of an employee must be accounted for when organizations consider personal information safeguards. Other lines of defense are critical.

[31] An MD Management protection measure that did not rely on the employee was the operating system's log-on password. There are various means of circumventing this password. Free software is available on the internet which may be downloaded onto a CD or floppy disk and inserted into the laptop to permit a thief to sign on as the computer's administrator and gain access to all locally-stored files. Microsoft gives instructions on how to bypass this log-on password and calls it the "weakest link" in securing a computing device. It advises on its website that log-on passwords are easily evaded:

The Weakest Link

Laptops are often the weakest link in the security chain, according to Munro:

- *BIOS passwords are easily bypassed on most machines.*
- *Even if it isn't, a thief can remove the hard disk and plug it into another machine.*
- *Once they have access to the disk, there are free programs on the internet that will figure out your Windows user name and password.*
- *From there, it's easy to crack locally stored VPN passwords, wireless network settings including encryption codes, locally cached email and anything else that is stored on the computer.*

⁶ <http://www.privacyrights.org/ar/ChronDataBreaches.htm>

- *In other words, without proper protection, if they own your laptop, they own your data. Game over!*

Proper Protection

So what does a properly protected laptop look like?

- *Choose laptops with ATA-3 BIOS passwords which are harder to circumvent and which lock the hard disk to the specific computer.*
- *Look for computers that include TPM (Trusted Platform Module) hardware.*
- *Make sure users actually set a BIOS password.*
- *Set up new laptops so that they can only boot from the hard disk.*
- *The most important thing is to use encryption on your data. Windows XP Encrypting File System does the business. You could also try PGP.*
- *For short, one-off secret files (e.g. a list of passwords) take a look at fSekrit. It turns text-only notes into encrypted files. It's also free.*
- *Ensure that the Administrator account has been renamed and given a strong password.*

A Sterling Tip

Encryption is vital. Although it is a bit fiddly to set up at first, it means that if your laptop is nicked, there are virtually no consequences apart from an insurance claim.⁷

[32] Data was encrypted in almost none of the cases of stolen laptops outlined earlier. Data encryption is a process used to obscure or scramble information to make it unreadable to unauthorized individuals. While PIPA does not prescribe specific safeguards, its federal counterpart, PIPEDA, specifies that:

The methods of protection should include

- (a) physical measures, for example, locked filing cabinets and restricted access to offices;*
- (b) organizational measures, for example, security clearances and limiting access on a “need-to-know” basis; and*
- (c) **technological measures, for example, the use of passwords and encryption** [Emphasis added][Principle 4.7.3, Schedule 1, PIPEDA].*

[33] Legislative requirements typically establish minimum standards for conduct. The fact that encryption is included as a safeguard in federal law suggests that it was considered by the legislators as an established measure of protection. It should be noted that MD Management is subject to PIPEDA in those provinces without provincial privacy legislation like PIPA.

[34] Other privacy commissioners have accepted that encryption is one reasonable safeguard for mobile computing devices. The Information and Privacy Commissioner of British Columbia recently recommended encryption after a public body sold computer tapes containing personal information. He stated:

For records in electronic form, consideration must be given to whether personal information is encrypted... in the United States, a number of states have laws that require organizations to notify individuals of security breaches affecting their personal information, but these requirements often do not apply to encrypted

⁷ www.microsoft.com/uk/businesscentral/newsletters/bulletins/laptop-security-advice-prevention-against-hacking.mspx. The OIPC does not advocate any specific brands of security measures. Some listed here are also not widely available.

personal information. This acknowledges the effectiveness of encryption as a means of addressing the risks associated with security breaches involving personal information. If personal information is properly encrypted, its security will be reasonably assured, even if the device or medium containing the information is improperly disposed of or acquired [Investigation Report F06-01].

[35] When an individual complained that inadequate safeguards were in place to protect employee drivers' licence numbers, the Privacy Commissioner of Canada found in PIPEDA Case Summary #107 that the organization's encryption of the data was a reasonable protection measure. The federal Commissioner made an identical finding in PIPEDA Case Summary #185 in which encryption of personal information was, again, deemed to be a reasonable safeguard.

[36] Microsoft Windows 2000 Professional is typically installed with 56 bit encryption. A no-cost upgrade to 128 bit encryption is available online. There are also other encryption applications which can be purchased or downloaded from the internet. Although the stolen laptop was equipped with a system that would secure files downloaded onto a specific area using Microsoft 2000 data encryption (128 bit DES), unfortunately, the file containing the personal information was not stored on this protected portion of the laptop. The Organization did not communicate this security feature to its employees in its policy.

[37] The risk of corporate laptops being stolen is well known and foreseeable. In most cases this occurs inadvertently: individuals naturally forget, become distracted or are outsmarted, victimized, swayed by convenience or may even apply their own acceptable risk threshold to a situation despite laptop handling policies. Although policies are necessary, without technical security measures that go beyond employee compliance, the likelihood that an unauthorized user could gain access to data stored on mobile devices is relatively high. Previous privacy findings as well as federal legislation recommend encryption as one reasonable measure of protection to guard against well known risks.

Seriousness of the Harm

[38] The sensitivity of personal information is a consideration in an assessment of harm and risk. PIPA does not delineate types of personal information as being more or less sensitive so as to demand more or less protection. However, it is acknowledged that certain types of personal information can be used to harm or perpetrate fraud against individuals more easily than other information. Other types of misuse of personal information may cause non-monetary harm by raising safety risks, damage to reputation, loss of reliability of information sources or trust in systems and individuals.

[39] I am of the view that "reasonable security measures" entails consideration for the possible harm to individuals if the information were in the wrong hands. PIPEDA explicitly recommends that organizations consider sensitivity when implementing security measures:

The nature of the safeguards will vary depending on the sensitivity of the information that has been collected, the amount, distribution, and format of the information, and the method of storage. More sensitive information should be safeguarded by a higher level of protection [Principle 4.7.2, Schedule 1, PIPEDA].

[40] The personal information on the MD Management laptop was, again:

- name
- age, month and year of birth (not *day* of birth)
- medical specialty
- home address and phone and fax numbers
- business address, phone and fax numbers
- home and/or business email address
- total financial assets with MD Management (in some cases)
- shareholder number (in some cases)

[41] The fact that total value of MD Management investment assets for each physician was listed causes some concern. Principle 4.3.4 of PIPEDA specifies that, like medical records, income records are “almost always considered to be sensitive”. A particular physician’s asset value could single him or her out as a target for burglary or varieties of fraud. I suggest that physicians, like many others, maintain unlisted home addresses and telephone numbers so as not to be disturbed at home. One type of fraud is identity theft, wherein an individual’s personal information is appropriated in order to commit fraud. Although definitions of identity theft differ, it ranges from subscribing to cellular telephone service in another person’s name to applying for loans and credit cards. The fact that SINs, investment account numbers and banking information was not present, in my view, lessens the seriousness of the potential harm to affected individuals since it is more difficult to commit serious fraud without that data. However, this information is not *required* to perpetrate identity theft.

[42] Phonebusters, a Canadian anti-fraud call centre operated by Ontario police agencies, received between 11,938 and 14,599 complaints of identity theft each year between 2003 and 2005⁸. The total annual financial cost to these consumers reached 20 million dollars. This does not include the time and money spent to rectify the problems created by identity theft. In March of 2006, an Ipsos Reid survey revealed that one-quarter of Canadian adults (24%) – representing roughly 5.7 million Canadians – have either themselves personally (4%), or know someone who has (20%), been subjected to identity theft⁹.

[43] In the United States, the Federal Trade Commission (FTC) reports that it received 255,565 identity theft complaints in 2005¹⁰. Based on its 2003 survey data, the FTC estimates that there were 10 million Americans victimized by identity theft that year¹¹. In this survey, the FTC calculates the average financial cost to a victim whose personal information is misused at between

⁸ http://www.phonebusters.com/english/statistics_E05.html

⁹ <http://www.ipsos-na.com/news/pressrelease.cfm?pid=2998>

¹⁰ “Identity Theft Victim Complaint Data: Figures & Trends January 1 – December 31, 2005”. Federal Trade Commission. January 2006.

¹¹ “Identity Theft Survey Report.” Federal Trade Commission. September 2003.

\$4,800 and \$10,000 USD, amounting to five billion dollars annually. In its definition of identity theft the FTC includes *actual* and *attempted* cases of credit card, phone, bank, employment, government documents/benefits, and loan fraud.

[44] In the event that the laptop thief or a purchaser of the stolen MD Management laptop was interested, the initial password could be bypassed with easily available instructions and the personal information could be used fraudulently. Again, the absence of the individuals' SIDs, complete date of birth, and other banking or credit card information would reduce the risk of the more serious or complex forms of identity theft.

[45] According to section 34 of PIPA, simply *enabling* the conditions for unauthorized access to information is a contravention of the Act; actual fraud need not occur. Beyond any harm caused by fraud, individuals also have fundamental rights to information privacy and to have their information protected by organizations. This is the purpose of PIPA, as outlined in section 3 of the Act.

[46] It should be noted that Edmonton area media immediately reported this incident and publicized the type of personal information on the stolen laptop. This media attention may have served to draw attention to the opportunities available to the laptop thief.

[47] In the current age, personal information is at greater risk to fraud than in the past. New varieties of fraud have become easier to commit, sometimes with even basic personal information, thereby increasing and altering the nature of potential harm to individuals. Identity theft data suggests that individuals are wise to be more cautious about disclosure of their personal information. Legislation reflects a shift in social policy and offers individuals a fundamental right to have their personal information protected by organizations to minimize potential harm.

Cost of Preventative Measures

[48] There were technical security measures available to MD Management at the time of the theft that would have been of minimal cost and of little effort. The Organization could have set up its laptops so that they could only boot from the hard disk and set up BIOS passwords and hard drive locks. These options, though by no means impenetrable, are often employed by single laptop users or smaller businesses and can be easily performed without significant cost to improve security.

[49] There are inexpensive and relatively straightforward encryption technologies which only allow data to be read with the correct password or key. Encryption of computer data generally falls into two categories: file-by-file encryption and disk encryption. Windows 2000 and Windows XP Professional have file encryption capability preinstalled that could have offered reasonable security in this case, had it been activated. Of course, some users find these

solutions to be cumbersome and impractical. Although the Organization had designed a variant of file-based encryption using the Windows' technology, it was not employed. Stronger file-by-file or disk encryption software is commercially available from a variety of vendors for between \$60 and \$150 per device. For the purposes of PIPA, any of these encryption safeguards would be considered reasonable.

[50] Encryption of these types may be more useful for individual computer owners or smaller businesses. Encryption technologies for larger-scaled organizations such as MD Management carries with it other issues and costs, particularly in large, integrated data and IT systems. Of course, larger organizations are still required to implement reasonable security arrangements, which should include an analysis of whether and how encryption technologies can be embedded within the broader data security arrangements of the firm, whether large or small.

[51] Tracking systems or "phone home" software for mobile devices that can trace the physical location of a laptop (even if the hard disk is reformatted and the operating system reloaded) are also available for roughly \$130 per device for three years of service. Some tracking systems are also offered with encryption, and the combination may be purchased in single quantities for approximately \$80 annually. These combinations create an encrypted partition on the hard drive. A thief can obtain access to the system and will appear to have wide use of it. However, he or she will not see any of the files in the encrypted partition because the system will not display that part of its directory. Meanwhile, "IP tracking" or even GPS location information signals are being sent to a "home" server each time the stolen laptop is connected to the internet.

[52] In order to retain control over data on a missing laptop, some organizations are examining a technology called a "kill switch". Similar to tracking services, a stolen laptop periodically connects with an Internet server. If the server notes that the laptop is flagged as stolen, it initiates a series of actions to prevent unauthorized access or sends "self-destruct" instructions. The "self destruct" command can also be set to proceed after certain events such as repeated failed password or authentication attempts, removal from pre-determined locations, travel further than preset distances, or connection via foreign or unauthorized networks. Single-user pricing for this service is less than \$200 annually per laptop.

[53] Finally, MD Management's laptop already had remote access capability ensuring that, once the user was logged on to the network, he would have had access to files stored on it. It would not always be necessary to maintain files on the laptop since they could be accessed remotely with a high speed connection. Proper network access security and authentication would offer a barrier for unauthorized users and access can be revoked quickly in response to the loss of a laptop.

[54] While the cost for different strengths, types and management strategies for data safeguards may vary, they are arguably less than an organization's cost

of recovering from a data breach. MD Management did not employ any of the measures described in this instance.

Relevant Standards of Practice

[55] When laptops are removed from an organization's site, they are more vulnerable to theft. The physical security arrangements that might be in place at many work sites - such as locked offices, entry pass cards or codes, security guards, building locks, and natural surveillance - are not in place. Even when these measures are in place, laptops still fall prey to thieves in the workplace because of their portable design which allows them to be removed inconspicuously from a worksite, compared to a desktop computer. As a result, laptop security is treated distinctly by data security professionals.

[56] Information technology experts routinely refer to "layers" of data security because they are less expensive, easier, and it is generally accepted that one protection measure is not likely to thwart a dedicated hacker. Applying layers of protection - administrative, physical and technical - requires significantly more effort and skill to penetrate, thereby reducing the risk of unauthorized access. An analysis of whether reasonable safeguards were in place should include examination of whether more than one of these layers was in place: physical security (as in locked cabinets, cable-locks, motion sensor/alarms, keeping devices in sight); administrative measures (as in behavioral rules and their enforcement, such as the policies to restrict the amount and type of data and time kept, "need-to-know" rules etc.); and technical protection measures (such as encryption, remote access, call-home and remote "kill switch" commands).

[57] MD Management employs a number of sound administrative controls such as ensuring that only authorized individuals have access to particular data and directing employees only to store information on their laptops that is required for an immediate task.

[58] Physical controls include MD Management's requirement that laptops not be left unattended (unless locked on the company site), and that they remain in sight lines. I have already addressed the issue of this being difficult to enforce. There are other physical measures available including laptop locking cables and safes. For example, after aerospace company Boeing had an unencrypted laptop stolen, it required employees to keep laptops physically locked to an immovable object at all times. Motion sensors, alarms, the laptop tracking software and "kill switch" mentioned are also available and bridge the gap between physical and technical solutions.

[59] Despite the laptop locking requirement, Boeing's proprietary and personal information is not permitted to be stored locally on laptops any longer. Instead, data can only be accessed remotely from company servers with multiple factor authentication. Boeing also conducts random laptop audits to ensure no forgotten files are contained on them. Of course, this requires that users always have high speed internet connection to conduct some of their business. Remote access is a good technical control but, if penetrated, could

give an intruder access to an organization's entire network. Authentication and access controls must therefore be rigorous and passwords should be immediately disabled if a threat is suspected.

[60] Basic technical measures include BIOS passwords, hard disk boot only, log-on and file password protection. Ensuring that the user is not also the laptop administrator helps prevent users from disabling some of these features. As discussed, another simple technical safeguard is encryption. In the United States, financial services company ING Group implemented a policy whereby no laptop can leave the premises without encryption software. After it experienced a laptop theft, Ernst & Young encrypted 30,000 company laptops. Even though Equifax policy now prohibits the storage of sensitive data on laptops, its laptops still require two levels of user authentication and have hard drive encryption.

[61] An organization need not implement each and every available security measure. However, it is well established that simple log-on passwords and employee watchfulness is insufficient. Organizations should apply multiple layers and measures that give personal information adequate protection. I have identified encryption as one possible technical safeguard because it is readily available and simple to use. In California, among other states, only stolen laptops with enabled data encryption are exempt from the requirement for organizations to notify affected individuals of the incident in which their personal information was compromised.

[62] Although long used by military intelligence, according to some research, encryption was in use by businesses even 10 years ago:

The use of encryption is expected to rise rapidly. Based on a survey of 1600 U.S. business users, the U.S. Chamber of Commerce, Telecommunications Task Force estimated that 17% of companies used encryption for confidentiality in 1995. They projected an annual growth rate of 29%, which would bring this figure to 60% by the year 2000. The 1996 Ernst & Young and Information Week annual security survey of 1300 information security managers found that 26% used file encryption, 17% telecommunications encryption, and 6% public-key cryptography¹².

This research likely overestimated the prevalence of encryption; a few years later, in 2001, *Information Week* and PricewaterhouseCoopers reported that 24% of companies worldwide were encrypting data for storage or transmission based on their survey of 500 companies¹³. Larger companies that have already experienced laptop thefts disproportionately move towards encryption. This should not dissuade smaller businesses from doing the same, as they are just as likely to be in custody of personal information. But, the private sector is not alone in the move to encryption; the U.S. government is in the process of encrypting data on all government mobile computers and devices. The Canadian government has already established this standard across federal departments:

Off-site use of departmental IT assets can introduce additional information security risks. Departments that allow personnel to access departmental information and IT

¹² Denning, Dorothy. "Encryption Policy and Market Trends", 1997.
<http://www.cs.georgetown.edu/~denning/crypto/Trends.html>

¹³ <http://www.informationweek.com/story/IWK20011011S0015>

assets, networks and systems from outside their government offices must establish procedures for such use.

To protect the remote computer, the information it contains, and the communications link, departments should use an effective combination of physical protection measures, access controls, encryption, malicious code protection (e.g. virus scanners), backups, security configuration settings (e.g. operating system controls), identification and authentication safeguards, and network security controls (e.g. a PC firewall).¹⁴

Encryption has fast become a baseline for security which has been influenced by the International Standards Organization which established, in section 11.7.1 of ISO 17799, that encryption is required to protect information stored on laptops:

*When using mobile computing and communicating facilities, e.g. notebooks, palmtops, laptops, smart cards, and mobile phones, special care should be taken to ensure that business information is not compromised. The mobile computing policy should take into account the risks of working with mobile computing equipment in unprotected environments. **The mobile computing policy should include the requirements for physical protection, access controls, cryptographic techniques, back-ups, and virus protection** [Emphasis added].*

[63] Information technology media has been full of articles about the importance of encryption on laptops. Recent incidents of corporate laptop thefts have solidified its relevance. This technology is already available on standard operating systems and can be easily obtained or purchased. Although decrypting an encrypted file is not impossible, it requires a high and rare degree of skill and time, making it a reasonable safeguard in the context of PIPA. Of course, organizations may consider any number or combination of the security measures discussed other than encryption.

VI. SUMMARY

[64] I find that MD Management did not comply with its duty under section 34 of PIPA to make reasonable security arrangements to protect the personal information contained on the laptop. I take this view based on the sum of the following:

- MD Management's laptop containing 8,000 individuals' personal information is or was in the custody of an unauthorized third party who stole it.
- The personal information contained on the laptop could expose the affected individuals to fraud. These individuals have a legislated right to information privacy and to have their information protected by reasonable safeguards.
- Under PIPA, MD Management is ultimately responsible for the conduct of the employee who, among other violations of policy, left the laptop unattended.

¹⁴ http://www.tbs-sct.gc.ca/pubs_pol/gospubs/TBM_12A/23recon-1_e.asp#Related

- Frequent incidents of laptop theft from employees, often despite corporate policies, are well known and publicized, making the risk real and foreseeable. MD Management’s policy recognized this risk, but did not adequately address it.
- Although MD Management had a policy in place prohibiting its employees from leaving laptops in their vehicles or unattended, relying on employees (who are fallible) as the main line of defense is not sufficient – especially given the availability of other security options.
- MD Management’s technical security measure in place was insufficient; a log-on password which can be circumvented using instructions that are easily obtained. This alone does not provide reasonable security.
- The operating system developer suggests that its password function does not offer adequate security and provides a preinstalled encryption feature as a standard option.
- Other available measures include cables and locks, motion sensors, alarms, laptop tracking software, remote data access (rather than local storage of data), “kill switch”, and more sophisticated encryption technology.
- Federal legislation and findings point to encryption as one recognized safeguard. This was not activated to encrypt the data stored on the stolen laptop.
- It is accepted that three layers of security are necessary: physical, administrative and technical. MD Management did not satisfy each layer.
- The International Standards Organization states that encryption should be a technical requirement for all mobile devices. Encryption has become one commonly used and accepted technical measure among organizations and governments who permit employees to remove personal information from the workplace on laptops.

[65] Although it is unknown whether the laptop thief has actually accessed, used or disclosed the personal information on the laptop, PIPA requires that organizations make reasonable security arrangements to protect against the potential for this occurring. For a breach of PIPA to occur, there is no requirement that actual unauthorized access, use or disclosure occur – just that the organization failed to comply with its duty to reasonably protect against the risk.

[66] In the present case, I find that MD Management contravened its duty to safeguard personal information in its custody, as required by section 34 of PIPA.

VII. OTHER CONSIDERATIONS

Post-Incident Action

[67] It should be noted that MD Management took the following action on its own initiative after the theft of the laptop:

- The Organization sent a notification letter dated June 29, 2006 to all affected individuals whose personal information was compromised. The letter explained that the matter had been reported to police and all of the actions taken by the Organization.
- Police were notified and a report was filed.
- The Organization requested both TransUnion and Equifax to place fraud warnings for five and six years on the affected individuals' credit profiles. This will alert credit grantors of the incident and urge them to notify the individual before extending credit. This measure will assist in reducing the likelihood that a fraudster could purchase items against the individual's credit.
- Both the Alberta Information and Privacy Commissioner and the Privacy Commissioner of Canada were advised of this incident.
- The Organization hired a security firm to conduct a private investigation and review its security arrangements and make recommendations.
- Employees were instructed to remove all client data from laptops until new security measures are in place.
- The Organization updated its employee training material to include further information about laptop security.
- MD Management is sending confirmation of transactions to its clients to verify that their transactions are legitimate. Extra scrutiny during phone transactions is also accomplished by asking identifying questions.
- The employee's supervisor spoke to the employee and placed a disciplinary letter on his file. He was advised that any further incidents could jeopardize his position.
- The Organization began examining and implementing enhanced security measures before this investigation was even completed.

[68] MD Management has been responsive to this incident and is taking the matter seriously. While this does not diminish the Organization's responsibility for the incident, I am of the view that it demonstrates how organizations should respond under similar circumstances.

VIII. RECOMMENDATIONS

[69] Given the steps already taken by MD Management, and under these circumstances, I recommend that the Organization take the following action:

1. Ensure that all laptops that contain personal information are equipped with data encryption capability that cannot be disabled by the user.
2. Remind employees of existing corporate "guidelines" which state that personal information on laptops must be limited to what is necessary, and the data may only be stored for as long as necessary to complete a task.
3. Codify the laptop "guidelines" in MD Management's formal policy. This should include explicit reference to the fact that data should be permanently deleted from laptops once it is no longer required.

4. Conduct a process audit to ensure that employees' access to personal information is limited to information required for the performance of the functions and duties associated with each position.
5. Conduct ongoing random laptop audits to ensure compliance with laptop policy.

[70] MD Management Ltd. agreed to adopt these recommendations; many were underway or were being examined before this investigation was complete. The Organization will complete installation of encryption software on all laptops by the spring. All staff have been given interim instructions about storage of sensitive data on laptops until the encryption solution is implemented and are receiving educational sessions about policy requirements. The Organization is in the process of formalizing enhanced laptop guidelines into policy and will conduct a functional role based analysis regarding employee access controls. Finally, MD Management will develop control tests and audit programs to ensure compliance with laptop policy. MD Management was cooperative throughout this process.

[71] The steps taken by the Organization meet PIPA's requirements to employ reasonable safeguards to protect personal information. I am of the view that it represents a sound course of action. This matter is considered resolved and the investigation is closed.

IX. CONCLUSIONS

[72] Organizations must carefully consider the safeguards in place to protect personal information contained on laptops and other mobile computing devices. A log-on password is not sufficient to satisfy the requirement for reasonable safeguards. While policy outlining who may store what data on a laptop and for how long is important, organizations should employ other physical, administrative and technical measures that do not rely strictly on employee compliance.

Preeti Adhopia, Portfolio Officer
Alberta Office of the Information & Privacy Commissioner