Norman P. Archer, Ph.D.
Professor Emeritus
Special Advisor, McMaster eBusiness Research Centre

1280 Main St. W. Ph. 905.525.9140 X23944
Hamilton, Ontario Fax 905.521.8995
Canada L8S 4M4 E-mail archer@mcmaster.ca

July 22, 2013

To Whom It May Concern

Concerning Mr. Mark LeBrun's Federal Court File T-132-13, dated June 28, 2013 re Canada Student Loans Case

Loss of the Canada Student Loans Program data in an unencrypted database, if the database has fallen into the hands of criminals, can result in a range of fraudulent uses of the data. Generally, these types of fraud can be classified into: 1) Existing account fraud, 2) New account fraud, and 3) Other fraud. In a 2008 survey of Canadian consumers[1], the annual rate of such fraud in the general population was found to be 6.1%, 0.2%, and 0.2% respectively. Details relevant to the Canada Student Loan case are discussed below.

1) It appears likely that the risk of existing account fraud is small, unless criminals can apply for student loan increases based on existing student accounts in the database and somehow divert the funds to their own use. The risk to fraudulent use of most other types of existing accounts such as credit cards is minimal, because relevant information about accessing such accounts was not included in the lost database.

2) There is a significant risk of new account fraud, since criminals could use student identity information contained in the lost database to apply for credit cards, mortgage loans, vehicle loans, and other types of credit. However, according to Mr. Mark LeBrun's affidavit, both of the credit agencies active in Canada (Equifax and TransUnion) have been contracted to insert a credit alert flag in the credit files of all those students who agree to this precaution and who have been affected by the loss of their personal identity data. As of June 21, 2013, 88,548 potentially affected persons had agreed to allow this to be done on their behalf. This is out of a total of approximately 583,000, or 15% of the students whose personal information was included in the unencrypted database that was lost. This can hardly be claimed to be blanket coverage of the people affected. Has HRSDC made provision for those individuals not covered by this plan if they suffer financially or otherwise as a result of the loss of the database?

2 (a) HRSDC has indicated a willingness to keep the credit alert plan in place for up to seven years. However, there is no time limit on criminal activities involving stolen identity information. Whether or not a student loan has been paid off, the lost identity information will still be out there, continuing to place the student at risk of fraud from sophisticated criminals. There has been little research into the length of time to be concerned about criminal use of stolen data. However, there is some experience in the United States on notification delays, where most of the States have enacted legislation concerning mandatory public notification about data breaches and delays in notification. In one data breach case, the State of Indiana Attorney General's office filed a lawsuit against *WellPoint Inc.*, claiming the health insurance provider did not notify its customers or the Attorney General's office in a timely manner

[1] Susan Sproule and Norm Archer, "Measuring Identity Theft and Fraud in Canada: 2008 Consumer Survey", McMaster eBusiness Research Centre Working Paper #23, July 2008.

following a data breach affecting thousands of customers. The lawsuit claimed that individuals potentially affected by a data breach were not notified "without unreasonable delay"[2]. The purpose of early notification is to give less opportunity for criminals in possession of the stolen information to make use of it for fraud. The lawsuit stated that "While most inadvertent security breaches do not result in fraud, notifying those affected in a timely manner significantly reduces the risk of identity theft, … Situations involving the theft of personal information for the purposes of identity theft most often result in some form of fraud occurring within seven to 10 days." Generally speaking, even though it is not possible to put a time limit on the criminal use of data that have been stolen, the risk of fraud occurring is highest in the early period after the theft event. It is important to note that, even if the Canada Student Loans database was originally only lost or misplaced, it could still fall into criminal hands at some point months or years in the future, so there would continue to be risk of fraudulent use of the data for some time.

2 (b) Whether or not the unencrypted database has fallen into the hands of criminals, flags on credit files will result in additional inconvenience to the persons participating in the credit alert program. Most of these individuals are at the beginning of their careers and will be making major purchases such as vehicles and homes over the next few years, with the majority of these purchases on credit. The firms asked to provide credit for major items such as these will almost invariably do credit checks and will find the credit flags. In order to safeguard their interests, these firms will then require additional meetings, identification, and references from the individuals applying for credit, resulting in further delays and frustration to the affected individuals.

3) The credit checks now in place will only detect criminal attempts to obtain credit by using information on individuals contained in the missing individual files. However, if the database has been stolen, the credit checks will not detect criminal attempts to use stolen information to apply for jobs, rent apartments or houses, open mobile telephone accounts, or to provide false background information to government agencies (e.g. tax information), or law enforcement agencies when charged with criminal or traffic offences. These activities will not usually result in credit checks by the vendor or agency, so credit file flags will not be effective. And if such activities occur, they may take a long time for victims to detect, often when they receive account or tax overdue notices for bills that the criminal has accumulated in the victims' names, or notices to appear in court. Historically, sorting out such a mess that is not of their own making can take a long time for victims, causing extreme distress as well as financial loss and wasted time and energy.

Sincerely,

Norm Archer, Ph.D.

[2] "WellPoint Sued For Delay In Disclosing Security Breach", http://www.darkreading.com/security/attacks-breaches/228200083/index.html