File No. CT 2005-006

COMPETITION TRIBUNAL

IN THE MATTER OF the *Competition Act*, R.S.C. 1985, c. C-34, as amended;

IN THE MATTER OF an application by B-Filer Inc, B. Filer Inc. doing business as GPAY GuaranteedPayment and NPay Inc. for an order pursuant to section 103.1 granting leave to make application under sections 75 and 77 of the *Competition Act*;

AND IN THE MATTER OF an application by B-Filer Inc., B-Filer Inc. doing business as GPAY GuaranteedPayment and NPay Inc. for an interim order pursuant to section 104 of the **Competition Act**.

BETWEEN:

B-FILER INC., B-FILER INC. doing business as GPAY GUARANTEEDPAYMENT and NPAY INC.

Applicants

- and -

THE BANK OF NOVA SCOTIA

Respondent

AFFIDAVIT OF JAMES F. DINGLE

I, **JAMES F. DINGLE**, of the City of the Ottawa, in the Province of Ontario, **MAKE OATH AND SAY**:

1. I worked at The Bank of Canada for 35 years, and a major portion of my career at the Bank of Canada was spent dealing with payment systems matters. I retired from the Bank of Canada in 2003. Since then, I have been employed by the International Monetary Fund as an expert in payment systems, and in particular as an assessor of security, efficiency and reliability of both paper-based and electronic payment mechanisms.

2. I have been asked by counsel to the Respondent, The Bank of Nova Scotia ("Scotiabank"), to provide an expert opinion relating to the regulatory and reputational risks if Scotiabank were to continue providing banking services to the Applicants.

3. I attach my report setting out my opinion on these issues as Exhibit **"A"** to this my Affidavit.

4. I attach a copy of my curriculum vitae as Exhibit **"B"** to this my Affidavit.

SWORN BEFORE ME at the City of Parry Sound, on Thursday, July ~~26~~ 27th, 2006.

Violet Warwick

Commissioner for Taking Affidavits

James F. Dingle

JAMES F. DINGLE

VIOLET ANN WARWICK, a Commissioner, etc.,
District of Parry Sound, for Joel W. Kennedy Professional Corporation, Barrister and Solicitor.
Expires March 27, 2007.

Professional Qualifications and Experience

1. A major portion of my 35-year career at the Bank of Canada dealt with payment-system matters. I have conducted research and published articles on the public policy implications of electronic funds transfers. I represented Canada on the Committee on Payment and Settlement Systems organized by the Bank for International Settlements, the committee charged with developing global standards for systemically important payment mechanisms.

2. The Bank of Canada appointed me Deputy Chairman of the Canadian Payments Association (CPA) in 1980, and I served the CPA Board in that capacity for over 20 years. As a result I was directly involved in the creation of numerous rules and standards for the clearing and settlement of various new types of payment items in Canada. Since retiring from the Bank of Canada in 2003, I have been employed by the International Monetary Fund as an expert in payment systems, and in particular as an assessor of the security, efficiency and reliability of both paper-based and electronic payment mechanisms. I have produced the assessments of the payment systems of Switzerland, the Czech Republic, Mauritania and Kuwait.

3. As a result of my experience at the Bank of Canada, the Canadian Payments Association, and with the International Monetary Fund, I am well-positioned to provide an opinion on a number of relevant banking issues raised in this case. Attached hereto is a copy of my Curriculum Vitae.

This is Exhibit "A-1" referred to in the affidavit of James F. Dingle, sworn before me, this 27th day of July 20 06

A Commissioner for taking Affidavits

VIOLET ANN WARWICK, a Commissioner, etc., District of Parry Sound, for Joel W. Kennedy Professional Corporation, Barrister and Solicitor. Expires March 27, 2007.

Material Reviewed

4. For the purposes of preparing this Report, I have reviewed the following documentation prepared by the Applicants and submitted to the Competition Tribunal:

(a) Affidavit of Raymond Grace affirmed June 15, 2005, and the Exhibits attached thereto;

(b) Second Affidavit of Raymond Grace affirmed September 1, 2005, and the Exhibits attached thereto;

(c) Affidavit of Joseph Iuso, affirmed August 29, 2005, and the Exhibits attached thereto;

(d) Third Affidavit of Aidan Hollis, sworn December 2, 2005;

(e) Third Affidavit of Patrick Healy, sworn December 2, 2005;

(f) Third Affidavit of Raymond Grace, sworn December 5, 2005;

(g) Fourth Affidavit of Raymond Grace, sworn December 5, 2005.

5. I have reviewed the following documents on behalf of the Respondent:

(a) Affidavit of Robert Rosatelli, sworn July 12, 2005, and the Exhibits attached thereto;

(b) Affidavit of David Metcalfe, sworn July 12, 2005, and the Exhibits attached thereto;

(c) Responding Affidavit of Robert Rosatelli, sworn September 21, 2005, and the Exhibits attached thereto;

(d) Affidavit of Robert Rosatelli, sworn November 25, 2005, and the Exhibit attached thereto;

(e) Affidavit of Ryan Woodrow, sworn November 24, 2005, and the Exhibits attached thereto;

(f) Affidavit of David Stafford, sworn November 25, 2005;

(g) Affidavit of Colin Cook, sworn November 23, 2005, and the Exhibits attached thereto;

(h) Affidavit of Douglas Monteath, sworn November 25, 2005, and the Exhibits attached thereto;

(i) Affidavit of Stanley Sadinsky, sworn November 22, 2005, and the Exhibits attached thereto;

(j) Affidavit of Christopher Mathers, sworn November 23, 2005, and the Exhibits attached thereto;

(k) Affidavit of Alex Todd, sworn November 25, 2005, and the Exhibits attached thereto;

(l) Transcripts from the examination for discovery of a representative of the Applicants, Raymond Grace, held on June 27 and 28, 2006.

Factual Overview

6. Having reviewed the above-noted material, I am aware of the following facts. Beginning in 1999, Raymond Grace approached the Soctiabank in Sherwood Park Alberta and opened a single account in the name of B-Filer Inc. o/a GPay. There appeared to be nothing untoward in relation to this account.

7. A further account was opened in the name of GPay on April 15, 2004. Six further accounts were opened in the name of GPay in June 2004.

8. Mr. Grace opened five further accounts in the name of B-Filer Inc. o/a GPay in October 2004. In November 2004, he opened 15 accounts in the name of NPay Inc. Thereafter, when he approached the manager of small business accounts, Ryan Woodrow, to open additional accounts because his business was growing, he was told by Mr. Woodrow that he would not open any further accounts for his business.

9. Thereafter, Mr. Grace was in contact with telephone banking and opened 80 accounts for his business over the ensuing 2 and ½ weeks beginning February 25, 2005.

10. The Branch was concerned about the number of accounts opened, and escalated the matter to head office in March 2005. The Branch Manager, Margaret Parsons,

recommended to Shared Services at Head Offices that the accounts be terminated. An investigation by Shared Services and others ensued, and a decision was made to terminate the accounts. In the intervening period, there were a number of reports from banking customers that money had been fraudulently removed from their accounts and transferred to the Applicants' accounts at Scotiabank.

11. As part of the investigation, Scotiabank learned something about the manner in which the Applicants were transacting business. For banking customers with accounts at Scotiabank, the Scotiabank customer would indicate on his or her computer, a desire to use the services of UseMyBank. The banking customer would be taken to UseMyBank's website and would be asked to disclose his or her bank card number and bankcard password. UseMyBank would then enter into the Scotiabank customer's account and direct a transfer funds from the customer's account to GPay as a bill payee on Scotiabank's list of bill payees. Once UseMyBank was in a position to confirm, having effected the transaction, that money had been transferred to GPay as a bill payee, UseMyBank then transferred funds from its own accounts or otherwise indicated to the recipient the funds would be forwarded. At some later time, the money directed from the customer's account to GPay as a bill payee would be released from Scotiabank's suspension account to the Applicants' account at Scotiabank.

12. For banking customers who did not bank with Scotiabank, the process employed by the Applicants was somewhat different. This banking customer, after entering UseMyBank's website, would be prompted to provide his or her internet password and bank card. UseMyBank would then enter into the bank customer's internet banking

website, enter the customer's password and bank card number, and would cause the funds to be e-mailed from the banking customer's account to the Applicants' at Scotiabank.

13. It is also apparent from materials that I have reviewed that the vast majority of funds, approximately 97% of all monies transferred, are being used for the purposes of internet gambling. In other words, the banking customer has instructed UseMyBank to remove funds from his or her account, with the Applicants directly or indirectly (through the casinos' management companies) funding those on-line gambling accounts.

14. Notice of Termination of banking services was given to the Applicants by letters dated May 11, 2005. Because of an outstanding injunction proceeding in Alberta, the accounts, as well as GPay's status as a bill payee on Scotiabank's list of bill payees, were ultimately terminated after the injunction was dismissed in September 2005.

Two Issues Considered

15. The purpose of this report is to express my opinions on two particular issues: Firstly, does the Applicants' business raise regulatory and reputational risks for Scotiabank. Secondly, did Scotiabank have valid business reasons for terminating the banking relationship with the Applicants.

Regulatory and Reputational Risks

16. Canadian banks conduct their affairs in a manner that is significantly constrained by legislation, regulation and supervision. The principal relevant laws are the *Bank Act*, the *Payment Clearing* and *Settlement Act*, and the *Canadian Payments Act*. These Acts are accompanied by detailed regulations covering particular areas of activity. The Office of the Superintendent of Financial Institutions (OFSI) supervises each bank, on an on-going basis, to ensure compliance.

17. One objective of this regulatory structure is to enhance the long-term viability of deposits at banks as the main medium of exchange for payment transactions throughout the economy. Most deposits at banks are easily transferable to third parties, for example by cheque, and hence comprise a large part of the national money supply.

18. Canada's banking system is generally viewed by its citizens and by those outside of Canada as a secure and stable banking system. In many respects, Canada's banking system is a model to the world. Tight regulatory control was one of the cornerstones to the building of Canada's banking system. Maintenance of this stringent control, including through new measures such as the Anti-Money Laundering Regulations and the OFSI guidelines, is of paramount importance to Canada's banking system.

19. Statistics from the Canadian Payments Association indicate that, as of 2005, 5.2 billion payment items totalling $4.53 trillion in transactions were cleared and settled through the Canadian payment system in 2005. Seventy-eight percent of the items cleared were electronic payments. On average, more than $164 billion worth of transactions were cleared and settled through the CPA systems every business day during 2005. In order to maintain this system, the regulatory framework must be strictly adhered to, to ensure that such payments are processed efficiently and safely.

20. Individual Canadians are usually prudent with respect to their bank deposits, realising the importance of avoiding any behaviour that would expose their money to theft. Banks, understandably, encourage such prudence. Trust among banks, and trust among individuals making and receiving payments, underpins bank deposits as the medium of exchange.

21. While some might view the tight regulatory controls as an unnecessary infringement on free enterprise, it is essential to look at the broader issues at stake. Tight regulation helps to mitigate risks inherent in a payment system that is responsible for the clearing and settlement of over $4.5 trillion annually.

22. In July 2005, the Canadian Payments Association produced a document entitled *A Guide to Risk in the Payment Systems Owned and Operated by the CPA*. In that document, the CPA reviewed elements of risk within the clearing and settlement system, and provided guidelines to Financial Institutions for minimizing the risk within the system. The authors of the paper note:

> *"It is important for all entities directly or indirectly involved in the business of payments to include risk management in their strategic planning process in order to ensure that the payments network is operating in a prudential and effective manner. All participants are responsible for maintaining the integrity of the system and understanding the implications of risk in the payment system.*[1]*"*

23. The same document goes on to define different types of risk that Financial Institutions are exposed to:

> (a) ***Reputational Risk*** *is the risk of significant negative public opinion that results in a critical loss of funding or customers. This risk may involve actions that create a lasting negative public image of, or loss of public confidence in, the overall operations of a Financial Institution or the payments system... An example of reputational risk may include unwanted publicity from a cyber attack on a Financial Institution's on-line banking network, thus affecting the confidence of users in the Financial Institution's payment service.*
>
> (b) ***Security Risk*** *... relates to intentional acts such as fraud, where a payment transaction is initiated or altered in an attempt to misdirect or misappropriate funds. This type of risk may also include other malicious acts or sabotage, such as hacking...which can leave a party subject to financial loss. There is also a risk to privacy when a third party illegally gains access to financial information... Security issues pose significant*

[1] *A Guide to Risk in the Payment Systems Owned and Operated by the CPA*, July 2005, p. 1

> *risks to the payments systems...[P]reventing, investigating, mitigating and recovering from security violations increase the cost to the payments system generally.*
>
> *(c)* ***Legal/Regulatory Risks*** *refer to the uncertainties or gaps in the legal/ regulatory framework.* [2]

24. The Applicants' business erodes the prudent behaviour of depositors as described below. As a result, it entails reputational, regulatory and legal risks for Scotiabank in at least four ways.

(a) **The Risk identified in the Canadian Payments Act and CPA Rules.**

25. Pursuant to the *Canadian Payments Act*, Scotiabank must be a member of the Canadian Payments Association, and must adhere to the CPA Rules. The Rules of the CPA govern the exchange, clearing and settlement of various types of payment items, and they have the force of law. Each Financial Institution is ultimately responsible for ensuring that the payment initiated by the end-user is cleared and settled in a safe, sound and efficient manner. Financial Institutions are "obligated to operate in the context of fulfilling the shared public policy objectives" of efficiency, safety and soundness.[3]

26. Rule E 2 deals with the exchange, clearing and settlement of electronic on-line payment items. On-line payment items include e-mail money transfers ("EMTs"). Section 5(a) of the Rule states that:

> *In all matters relating to the Exchange, Clearing and Settlement of On-line Payment Items for the purposes of Clearing and Settlement, each Member shall respect the privacy and confidentiality of the Payer and Payee.*
>
> ...

---

[2] *A Guide to Risk in the Payment Systems Owned and Operated by the CPA*, July 2005, pp. 9-10
[3] *A Guide to Risk in the Payment Systems Owned and Operated by the CPA*, July 2005, p. 19

> *For greater clarity, the Payor's* [i.e. the banking customer's] *personal banking information, such as but not limited to the authentication information (e.g., user identification and password) and account balance,* ***shall not be made available at any time to the Acquirer and/or Payee*** [i.e. the Applicants] *during the On-line Payment Transaction session.*

27. Prior to Scotiabank's termination of the Applicants' banking services, whenever Scotiabank received an on-line payment item from another CPA Member in the daily clearing process, if that item is produced by actions of the Applicants and their joint venture partner UseMyBank, the Payer's account identification and password was revealed to UseMyBank. The Applicants have confirmed that it is impossible to carry on their business without the banking customer providing this confidential information to the Applicants.

28. If Scotiabank were required to continue to offer banking services to the Applicants, now knowing that it is the Applicants that are authenticating the transaction, Scotiabank either has to clear the EMTs received from other CPA members in breach of Rule E2, or not clear any of the on-line payment items (EMTs) transferred into the Applicants' Scotiabank accounts.

29. In my opinion, Scotiabank would be put in an untenable position. In order to offer banking services and clear and settle the transactions into the Applicants' accounts, it would be forced to do so in violation of Rule E2. Such a violation would pose both a regulatory and a reputational risk to Scotiabank. Scotiabank could be subject to a compliance proceeding for breach of Rule E2. As well, a failure on the part of Scotiabank to abide by the CPA Rules for clearing and settlement would reflect very negatively upon Scotiabank's reputation and business.

(b) **The Risk identified in the OSFI Guideline on Money Laundering, etc.**

30. The Office of the Superintendent of Financial Institutions ("OSFI") is the primary regulator and supervisor of all Banks in Canada. Its mission is to safeguard depositors and others from undue loss. OSFI is created by statute. One of the purposes of the *Office of the Superintendent of Financial Institutions Act* is to ensure that financial institutions are regulated by an office of the Government of Canada, so as to contribute to public confidence in the Canadian financial system. One of the objects is to promote the adoption by financial institutions of policies and procedures designed to control and manage risk. The Act includes penalties for contravention by a financial institution of orders or directions made by OSFI.

31. In April 2003, the Office of the Superintendent of Financial Institutions issued a Guideline on sound business and financial practices for "Deterring and Detecting Money Laundering and Terrorist Financing". The Guideline identified some of the steps that federally regulated Financial Institutions should take to minimise the possibility that they could become a party to such illegal activities, and to assist their compliance with the various legal requirements.

32. One requirement is the reporting of suspicious transactions likely to involve money laundering or terrorist financing activities (MLTFA). OSFI expects that institutions will be able to demonstrate that they have developed policies and procedures to deter and detect MLTFA, and that staff are applying them as intended.
As stated by Christopher Mathers in his affidavit, the Applicants are operating a money services business as defined by the *Proceeds of Crime (Money Laundering) and Terrorist*

Financing Act. Providing banking services to Money Services Businesses carries with it both enhanced risks and enhanced record keeping and reporting requirements.

33. OSFI requires Financial Institutions, including Scotiabank, to comply with their obligations. If Scotiabank failed to meet its obligations as set out by OSFI, in my experience, this could pose a significant reputational risk for Scotiabank in addition to exposing Scotiabank to a fine under the *Office of the Superintendent of Financial Institutions Act*.

(c) **The Risk of violating the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act***

34. The *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (PCMLTFA) implements various measures to detect and deter these activities, establishing record keeping and client identification requirements for financial service providers, and requires that banks and other financial entities report suspicious transactions as well as the cross-border movements of currency and monetary instruments.

35. Following investigations undertaken by various groups at Scotiabank, Scotiabank learned that Canadians gambling at internet off-shore casinos were able to initiate transfers of their funds on deposit at Canadian banks, routing the transfers to Scotiabank via on-line payments or bill payments to Applicants' accounts. The Applicants' then facilitated the funding of accounts at off-shore casinos used by Canadian banking customers for off-shore internet gambling.

36. In these circumstances, the *PCMLTFA* imposes record-keeping and reporting obligations. If Soctiabank failed in its record keeping or reporting obligations under the

PCMLTFA, this would create both a regulatory and a reputational risk for Scotiabank. The regulatory risk is set out expressly in the legislation, providing for significant fines in the event of a conviction under that Act. The reputational risk arises because as such a breach would result in a loss of public confidence in Scotiabank and would create a negative impression of Scotiabank's attention to regulatory concerns.

(d) **The Risk of violating the *Criminal Code***

37. I have had an opportunity to review the opinion of Stanley Sadinsky. I understand from that opinion that, pursuant to section 21 of the Criminal Code, one party commits an offence when aiding and abetting a second party that is committing a criminal offence. Scotiabank has been advised that Canadians located in Canada who are engaged in off-shore internet gambling are very likely committing an offence under section 202 of the Criminal Code. Moreover, under section 201(1)(c) of that Code, it is an offence to have under one's control any money relating to a transaction that is an offence under section 202.

38. The Applicants had over 100 Scotiabank accounts, which were used to receive money being transferred by gamblers to fund gambling accounts at off-shore casinos. The regulatory and reputational risks for Scotiabank in continuing to provide banking services to the Applicants who are facilitating off-shore gambling and who themselves may be engaged in the commission of a criminal offence are significant. Even where there is a debate concerning whether that activity is illegal, in my opinion, a Financial Institution such as Scotiabank, would be justified in terminating its banking relationship in these circumstances.

(e) Risk of Unauthorized or Fraudulent Transactions

39. One of the risks associated with electronic transactions – as in any payment - is the risk of unauthorized or fraudulent transactions. The Financial Institution must always take sufficient action to be as confident as possible that the debit has been properly authorized by the banking customer. In the case of electronic transfers of funds, authentication of the customer's identity is particularly difficult.[4]

40. The Applicants manner of conducting business, which requires banking customers to disclose their bank card number and secret internet banking password exposes Scotiabank to actual or claimed unauthorized or fraudulent transactions. Despite the Applicants' assertion that their system is secure, Alex Todd in his affidavit points out a number of shortcomings in the Applicant's security system, including statements made on UseMyBank's website which suggest that customer internet banking password information is stored. According to Mr. Todd, there is always a risk that, where password information is being collected, the system could either be hacked into or information could be obtained by a dishonest employee.

41. In these circumstances, if banking customers' password information were improperly accessed either from the inside or from the outside, there could be a breach of security for the banking customers that have used the Applicants' services. The Applicants state in their materials that 20,000 Canadians have used their services. A security breach involving a population of this magnitude could have a significant financial impact not only on thousands of banking customers, but on Scotiabank,

---

[4] *A Guide to Risk in the Payment Systems Owned and Operated by the CPA*, July 2005, p. 36

particularly in circumstances where it continued to provide banking services knowing that the Applicants are requiring the disclosure of information.

42. Moreover, there is the risk that banking customers who did authorize UseMyBank to remove money from their accounts might later claim that such transfers were not authorized. Mr. Grace has described this in his affidavits as "buyer's remorse". Given that the vast majority of the transactions conducted by the Applicants relate to off-shore internet gambling, there is a real risk that banking customers who actually authorized the transaction will later dishonour the instructions and claim that the transaction was fraudulent. Less obvious are the significant internal costs associated with Scotiabank and any other Financial Institution involved investigating each incident of an actual or asserted fraudulent transaction.

43. The reputational risk to Scotiabank, if it was knowingly increasing the chances of unauthorized disclosure, would be substantial. Moreover, whenever a high profile breach occurs where there is unauthorized use of banking customers' passwords, the banking system-wide effect is to undermine the confidence in the electronic banking system generally.

Business Reasons for Terminating the Banking Relationship

44. Scotiabank had at least five valid business reasons for terminating its banking relationship with the Applicants. In my opinion, none of these reflected an effort to gain market share.

45. Because there is some overlap in this section with the regulatory and reputational risks discussed in the preceding section, I will provide my opinions succinctly in relation to these business reasons:

(a) **A Reduction in the Security of Certain Bank Deposits at Major Institutions**

46. Payers (including gamblers) using UseMyBank are required to reveal their internet banking password and bank card number to the Applicants. This requirement would force such banking customers with Scotiabank (and indeed with most major Canadian banks) to violate their account agreements. Such carelessness with respect to the use of passwords, etc., could be expected to cause a rise in fraudulent transactions. These would require investigation by the staffs of the relevant banks, and appropriate attention to the needs of the depositors involved.

(b) **A Potential Decline in the Trustworthiness of Scotiabank in the Payment Clearings**

47. Scotiabank, when receiving on-line payment items (EMTs) from other institutions in the daily clearings established for such items by the Canadian Payments Association, would be in violation of CPA Rule E 2 whenever the items resulted from the operations of UseMyBank.

48. Mutual trust among banks and other clearing institutions that each is following the CPA Rules is essential in order for the Canadian clearing system to operate safely and efficiently. A failure comply with CPA Rule E2 could undermine Scotiabank's reputation amongst the other banks.

(c) **The Applicants' Business was No Longer "Small"**

49. Banks often attempt to control the risks involved in providing services to various types of clients by developing appropriately prudent policies to manage risk. As a general rule, a "large" client, however a particular bank defines it, has the potential to cause greater harm than a "small" client.

50. Scotiabank uses ceilings on the cumulative number and value of deposits each month (among other measures) to determine if that client is small or large. The Applicants opened over 100 deposit accounts in Scotiabank, and redirected the flow of incoming deposits from one such account to another when the cumulative value and/or number of deposits approached the ceilings set out in the Scotiabank banking agreements governing each of these "small business" accounts.

51. In my opinion, a Financial Institution must make a prudent judgment concerning the risks arising when a particular products and services are offered to a business customer, based on criteria developed by the Financial Institution. Where the Applicants' business exceeded the small business criteria, Scotiabank was justified in making a business decision not to offer to the Applicants small business accounts or other services usually offered to small businesses such as EMTs.

(d) **The Applicants operate a "Money Service Business"**

52. The *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* defines a Money Service Business as:

> *A person or entity that is engaged in the business of remitting funds or transmitting funds by any means or through any person, entity or electronic funds network, or of issuing or redeeming money orders, traveller's cheques or other similar negotiable instruments. It includes the financial entity when it carries out one of these activities with a person or entity that is not an account holder.*

53. The Applicants, together with their joint business venture UseMyBank, transmit the funds of individuals gambling at off-shore internet gambling sites, using email money transfers (EMTs) and electronic bill payment. The Applicants and UseMyBank are a financial entity that carries out such transmissions for banking customers and merchant customers (i.e. often casinos or their management companies) who do not hold accounts with Scotiabank.

54. According to the evidence of Christopher Mathers, under the provisions of the above Act, Scotiabank would be required to keep a record of the name, address and the occupation of each payer (gambler) and each merchant customer. This would involve a very labour-intensive effort on the part of Scotiabank, and would require the full cooperation of each bank from which a payer's EMT came.

55. In my opinion, the resources needed to assemble the required information on approximately 20,000 individual payers would easily justify a decision on the part of Scotiabank to stop providing services to the Applicants.

56. Moreover, the incoming transfers to the deposit accounts of the Applicants may constitute suspicious transactions, given their questionable legality. Each transaction would thus need to be reported to the federal agency FINTRAC established pursuant to the PCMLTFA.

57. In my opinion, the termination of the banking relationship in the light of these substantial requirements represents a prudent rational response to a costly and risky situation.

(e) **The Applicants' are likely Facilitating Illegal Activity**

58. Scotiabank's investigation beginning in March 2005 of the activity in the Applicants' deposit accounts revealed a number of warning signs concerning the Applicants' business. There was the very rapid growth over a single year in the volume and value of deposits being made to Applicants' accounts. Rapid growth is a recognized sign of money laundering.

59. Moreover, a number of the on-line payment items (EMTs) reaching Scotiabank for credit to Applicants' accounts were challenged by payers as being fraudulent, in the sense that the payers denied authorizing the transfers.

60. This pointed in the direction of illegal activity -- and raised several of the significant reputational and legal risks for Scotiabank described above -- as long as the Applicants' accounts were still in use. Scotiabank terminated its banking relationship with the Applicants and closed the Applicants' deposit accounts in order to avoid becoming a knowing party to such activities. In my opinion, in these circumstances, Scotiabank had a legitimate business reason for terminating its banking relationship with the Applicants.

Conclusions

61. In my opinion, Scotiabank faced significant regulatory, legal and reputational risks as long as it continued to provide banking services to the Applicants. The risks are summarized as follows:

(a) There is a significant risk of ongoing claims by banking customers that certain transactions in their accounts were not authorized, as well as a material risk that either a dishonest employee or a computer hacker could gain access to the 20,000 internet banking passwords and cause a

substantial damage to the reputation of Scotiabank and of the Canadian Payments Systems.

(b) Continuing to provide banking services to the Applicants while knowing that the vast majority of payments are being transferred from banking customers, to the Applicants' Scotiabank accounts, and ultimately to off-shore casinos or their management companies raises serious issues with respect to legality of the actions of the banking customers and also the actions of the Applicants, placing Scotiabank's reputation at risk in the event that it was required to continue to offer banking services;

(c) Failure to comply with the OSFI guidelines, including the guidelines relating to "deterring and detecting money laundering and terrorist financing" could result in enforcement proceedings as well as damage to Scotiabank's reputation;

(d) Similarly, failure to implement the rigorous PCMLTF record keeping obligations that would arise in these circumstances, requiring Scotiabank to keep a record of the name, address and principal occupation of numerous banking customers using UseMyBank, as well as the merchant customers to whom the money was being directed, could result in regulatory proceedings as well as damage to Scotiabank's reputation; and

(e) Continuing to participate in the clearing of funds transferred to the Applicants' Scotiabank accounts would be in breach of CPA Rule E2, and would pose specific regulatory and reputational risks;

62. It is my opinion that Scotiabank had numerous valid reasons for terminating its business relationship with the Applicants. The reasons were assembled in the course of the internal investigations. In my opinion, Scotiabank's decision to terminate banking services to the Applicants was entirely appropriate, given the significant reputational and regulatory risks associated with continuing to offer banking services to the Applicants.

James F. Dingle

13 Linden Terrace
Ottawa, On K1S 1Z1
Canada

Tel. (613) 232 7587
Fax (613) 232 4189
jimdingle@sympatico.ca

Citizenship: Canadian
Date of birth: 3/6/41

Professional profile: Knowledgeable and experienced in monetary and financial matters, especially central banking, monetary policy operations, money markets, clearing and settlement systems, and payment systems. Involved in both the formation and application of the Core Principles for Systemically Important Payment Systems. Fluent in English and French; generally competent in reading and speaking German.

Education: University of Toronto, Bachelor of Commerce, 1964.
Massachusetts Institute of Technology, PhD, 1968.

Career History: University of Toronto. Lecturer in Monetary Economics, and in International Economics. 1967-1968.
Bank of Canada, Ottawa. Increasingly responsible positions in the Research Department, the International Department, the Securities Department, and the Department of Monetary and Financial Analysis. 1968-2003. A senior officer of the Bank from 1981 until retirement in 2003.
Bank for International Settlements, Basel. Secondment from the Canadian central bank to the BIS Monetary and Economic Department, conducting research on the public policy implications of electronic systems for funds transfers.
Canadian Payments Association, Ottawa. Deputy Chairman of the Board of Directors, 1980- 2003. Consensus builder and architect for the development of Canada's large-value funds transfer system.
International Monetary Fund, Washington. 2001-2004. Participation in the Financial Stability Assessments (FSAPs) of the Czech Republic, Switzerland, Kuwait and Mauritania as the expert applying the BIS Core Principles for Systemically Important Payment Systems. Participation in the IMF Technical Assistance mission to Albania in 2004 with respect to the operation of its real-time, gross settlement, payment system. Participation in the FSVC mission to Morocco in 2004 to prepare an implementation plan for a real time gross settlement (RTGS) system.

Other Interests: Married with three daughters.
Cellist in the Ottawa Symphony Orchestra, 1968-2006.
Member of the Administrative Council of L'Eglise Christ-Roi, Ottawa, 1970-1986.
Active racer of small sailboats.

"B"

This is Exhibit B *referred to in the affidavit of* James F. Dingle *sworn before me, this* 27th *day of* July *20* 06

A COMMISSIONER FOR TAKING AFFIDAVITS

VIOLET ANN WARWICK, a Commissioner, etc., District of Parry Sound, for Joel W. Kennedy Professional Corporation, Barrister and Solicitor.
Expires March 27, 2007.

BETWEEN:

B-FILER INC.
Applicants

- and -

THE BANK OF NOVA SCOTIA
Respondent

Court File No. CT 2005-006

COMPETITION TRIBUNAL

AFFIDAVIT OF
JAMES F. DINGLE

McCarthy Tétrault LLP
Barristers & Solicitors
Box 48, Suite 4700
Toronto Dominion Bank Tower
Toronto, ON M5K 1E6

F. Paul Morrison LSUC #: 17000P
Tel: (416) 601-7887
Fax (416) 868-0673

Lisa M. Constantine LSUC#: 35064B
Tel: (416) 601-7652
Fax: (416) 868-0673

Solicitors for the Respondent

4106090 v.1