

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:

COMPETITION TRIBUNAL
TRIBUNAL DE LA CONCURRENCE

FILED / PRODUIT

June 22, 2006

Jos LaRose for / pour
REGISTRAR / REGISTRAIRE

OTTAWA, ONT

0105

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

Applicants

- and -

THE BANK OF NOVA SCOTIA

Respondent

**RESPONSE TO AMENDED NOTICE OF APPLICATION
PURSUANT TO SECTION 75 OF THE COMPETITION ACT**

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

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

Glen G. MacArthur LSUC# 13669A
Tel: (416) 601-7888

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

Solicitors for the Respondent, The Bank of Nova
Scotia

TO: **THE REGISTRAR**
Competition Tribunal
The Thomas D'Arcy McGee Building
90 Sparks Street, Suite 600
Ottawa, ON K1P 5B4

Tel: (613) 957-7851
Fax: (613) 952-1123

AND TO **SHERIDAN SCOTT**
Commissioner of Competition
Competition Bureau
50 Victoria Street
Gatineau, QC K1A 0C9

Tel: (819) 997-3301
Fax: (819) 953-5013

AND TO: **AFFLECK GREENE ORR LLP**
Barristers & Solicitors
One First Canadian Place
Suite 840, P.O. Box 489
Toronto, ON M5X 1E5

Michael Osborne LSUC# 40976K
Tel: (416) 360-5919

Jennifer L. Cantwell LSUC# 49515F
Tel: (416) 360-1485
Fax: (416) 360-5960

AND TO: **EDY, DALTON**
Barristers & Solicitors
800-1015 4 Street S.W.
Calgary, AB T2R 1J4

Sharon J. Dalton
Tel: (403) 263-3200 ext. 105
Fax: (403) 263-3202

Solicitors for the Applicants

I. OVERVIEW - SCOTIABANK OPPOSES THIS APPLICATION

1. The Bank of Nova Scotia (“Scotiabank”) admits the grounds and material facts in paragraphs 1, 6, 7, 8 12 and 13 of the Amended Notice of Application.

2. Except as otherwise admitted, Scotiabank denies the grounds and material facts in the Amended Notice of Application.

(a) The Parties

3. The Bank of Nova Scotia (“Scotiabank”) is one of Canada’s major Schedule I chartered banks. Scotiabank began serving customers in the Halifax area in 1832. Since that time, Scotiabank has grown to one of the largest Banks in Canada, with branches and offices in 50 countries and 50,000 employees worldwide.

4. As one of Canada’s Schedule I Banks, Scotiabank is regulated by the *Bank Act*. Schedule I Banks, including Scotiabank, must meet strict regulatory requirements. Scotiabank’s principal regulators in Canada are the Office of the Superintendent of Financial Institutions, the Financial Consumer Agency of Canada, and the Canadian Deposit Insurance Corporation. Scotiabank is also subject to laws of general application within Canada, including but not limited to the *Canadian Payments Act*, the *Competition Act*, the *Criminal Code*, the *Personal Information Protection and Electronic Document Act*, and the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*.

5. One of Scotiabank’s paramount responsibilities is to keep customers’ financial and personal information secure. The confidentiality of each customer’s electronic signature, which includes the customer’s PIN and Internet banking password, is one of the cornerstones to protecting the electronic banking system from fraud and thereby maintaining customer confidence in the system.

6. Raymond Grace is the President of NPay Inc. (“NPay”) and B-Filer Inc. (“B-Filer”) and the CFO of UseMyBank. B-Filer carries on business as GPay. NPay, GPay, and UseMyBank are operating as a single business enterprise. By using customers’ confidential Internet banking passwords, the Applicants effect transfers of funds from banking customers’ accounts to the Applicants’ accounts at Scotiabank. The Applicants then transfer the funds to off-shore Internet casinos. Approximately 98% of the Applicants’ business relates to transfers of funds from Canadian banking customers’ accounts to off-shore Internet casinos or their management companies.

(b) Background Summary

7. The Applicants first opened an account at Scotiabank in 1999 as a small business customer. They are operating a single business enterprise. They are no longer a small business. The volume of transactions passing through their accounts now far-exceed the small business limits of \$400,000 per month in deposits, or a maximum of \$5 million per year in deposits.

8. The following is a brief summary of the Applicants’ banking relationship with Scotiabank:

(a) Prior to April, 2004, the Applicants had opened only a single account at Scotiabank for the conduct of their combined business.

(b) Between April 2004 and March 2005, the Applicants caused to be opened a further 108 small business accounts at Scotiabank. The manner in which these accounts were opened was in violation of numerous Bank policies. Further, Mr. Grace made material misrepresentations upon which Scotiabank relied in permitting the accounts to be opened.

(c) Scotiabank had undertaken preliminary investigations of GPay in its capacity as a bill payee in 2001 and 2003. Those investigating GPay had concerns about the fact that GPay was requesting customer password information. However, only a few

Scotiabank customers were using GPay at the time. As a result, the decision was made to deal with the matter by speaking directly to the customers using GPay and warning them about the dangers of disclosing their bank password.

- (d) Scotiabank was not fully aware of the true nature and extent of the Applicants' business and the manner in which it was using Scotiabank's accounts until it undertook a comprehensive investigation of the Applicants' business and accounts beginning in early 2005.
- (e) As a result of this investigation, Scotiabank concluded that the Applicants' business raised serious business, legal, policy and reputational concerns for Scotiabank. Scotiabank's Security and Investigation Group learned that in the preceding 12 months, the Applicants had transferred almost \$10 million through their Scotiabank accounts. The magnitude of the Applicants' business that they were transacting through their Scotiabank accounts and the number of banking customers that were using their services had significantly increased compared to the situation in 2003, when it involved a small handful of Scotiabank customers. Scotiabank was no longer willing to provide banking services to the Applicants, because:
 - (i) the vast majority of transactions processed by the Applicants involve transfers of money to offshore Internet gambling casinos, which is most likely illegal;
 - (ii) the business model of the Applicants requires Scotiabank's customers to disclose their confidential on-line banking password which constitutes a serious breach of Scotiabank's Internet banking security and exposes Scotiabank and its customers to serious risk of fraud;

- (iii) the Applicants' business is a "Money Services Business" as described in the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*, which imposes enhanced due diligence, record keeping and reporting obligations on Scotiabank;
- (iv) the Applicants, who purport to be acting as "agents" for the banking customers in entering the banking customers' accounts, are transferring money out of these accounts to the Applicants' Scotiabank accounts. Scotiabank has legitimate concerns that the Applicants' Scotiabank accounts are being used "by or on behalf of third parties" as contemplated by the Regulations that are made pursuant to the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*. This creates very onerous record keeping obligations for Scotiabank, which Scotiabank is not prepared to undertake. Nor is Scotiabank prepared to bear the regulatory and reputational risks that the Applicants' Scotiabank accounts could be used by unscrupulous individuals to launder money or finance terrorist activity.
- (v) the Applicants no longer qualify as a small business, and, based on the information gathered during the investigation by Scotiabank, would not have been accepted as a commercial customer of Scotiabank; and
- (vi) the rules of the Canadian Payments Association (the "CPA") and, in particular, Rule E2, prohibit Scotiabank from clearing items in circumstances where the banking customer's authentication information, such as user identification and password, have been made available to the payee, which is the case for all transactions processed by the Applicants.

Thus, Scotiabank terminated the accounts of the Applicants for valid and legitimate business, regulatory policy and legal reasons.

(c) Applicants' Money Transfer Methods Breach Bank Security

9. Prior to the termination of the Applicants' banking services by Scotiabank, the Applicants effected the transfer of money from bank customers' accounts in two ways. The first was through Scotiabank's Bill Payment system. The second was through the use of e-mail money transfers ("EMTs"). For both methods, banking customers are required to breach their Cardholder Agreement with Scotiabank by disclosing their confidential bank card number and Internet banking password. Through both methods, the banking customer is able to remain anonymous with respect to the fact that they are transferring money to an off-shore on-line casino. Their bank statement would simply show that they had transferred money to "GPay" either by way of the Bill Payment system or through an EMT.

(i) The Bill Payment Method of Transfer

10. Using the first method, Scotiabank customers are required to provide their confidential bankcard number and on-line banking password to UseMyBank. The Applicants then enter into the customer's Scotiabank account as if they were the customer and cause money to be transferred from the customer's Scotiabank account to GPay as a bill payee.

11. The Applicants then notify the "merchant", most often an offshore Internet casino, or the casino's management company, that the money has been transferred from the banking customer's account, which in turn allows the banking customer to gamble online almost immediately. All of this occurs before the Applicants have actually received the money through the bill payee system. Because they themselves have actually effected the transaction, the Applicants have certainty that

the money is on its way, and they can therefore notify the on-line casino to permit the banking customer to gambling.

12. As with all bill payees, money that is directed to the bill payee on a given day is held in a Scotiabank suspension account until 8:30 p.m. each evening. The money is then released from the Scotiabank suspension account and directed to the bill payees' bank accounts.

13. In the case of GPay, the money was directed to the Applicants' accounts at Scotiabank (that had been designated to receive bill payments) or to GPay's account at another Financial Institution. The Applicants later transfer the money to the off-shore Internet casino or the casino's management company, after deducting a fee for the service that they have provided in acting as the transferor of money between the banking customers' bank accounts and the Internet casino.

(ii) The EMT Method of Transfer

14. The second method by which money is transferred involves customers who bank at Banks other than Scotiabank. Here too, the banking customers are required by the Applicants to divulge their confidential bank card number and Internet banking password.

15. The Applicants then enter the customer's Internet banking site and cause money to be e-mailed to one of the Scotiabank MoneyMaster accounts held by the Applicants.

16. Once the Applicants know that the money has been emailed from the banking customers' accounts, they notify the Internet casino (or the casino's management company) that the transfer has been made, so that the banking customers can then gamble online.

17. At some later point, the Applicants would accept the email money transfers into one of their 100+ Scotiabank accounts. Thereafter, at certain intervals, they would withdraw monies from their Scotiabank accounts and deposit these monies in their account at another Canadian financial

institution. From these accounts, the Applicants would transfer money to the off-shore casinos or their management companies, after taking a deduction for the service that the Applicants provided in acting as the transferor of monies between the banking customer and the off-shore Internet casino.

(d) Termination of Banking Relationship with Applicants

18. The business enterprise of the Applicants is one for which Scotiabank is not prepared to allow its accounts and services to be used. Scotiabank terminated its services to the Applicants due to legitimate legal, regulatory, business and reputational concerns, which have nothing to do with competition. Most importantly, as noted in Justice Simpson's Reasons for Previous Order, dated November 14, 2005 granting leave to apply under section 75 of the *Competition Act*, at para. 34:

"34. There is no doubt that the vast majority of Purchasers who use the Applicants' Business are paying amounts owed to offshore internet casinos. I have reviewed sections 202 and 207 of the Criminal Code, R.S. 1985, c. C-46, and have concluded that paragraph 202(1)(e) could make it an offence for a person in Canada to make an agreement on the internet as a prelude to gambling at an offshore internet casino ..." [emphasis added]

19. Scotiabank has serious and valid concerns about the legality of the activities of the "vast majority" of the users of the service provided by the Applicants. It is not willing to allow its facilities to be used for activities that could be illegal. The association of the Scotiabank brand with the activities of the Applicants could be interpreted by Scotiabank customers as an endorsement of the Applicants' service or suggest legitimization offshore on-line gambling.

20. Moreover, Scotiabank is concerned that banking customers who use the Applicants' services are disclosing their confidential Internet bank password to the Applicants. This poses security risks for the banking customers, and the banking system, in that either a rogue employee or a computer hacker could gain access to the Applicants' computer files and therefore access to the banking

customers' accounts. Not only does this pose a risk for Scotiabank's customers, it also poses an unacceptable reputational risk for Scotiabank.

21. By letters dated May 11, 2005 Scotiabank exercised its contractual right to terminate its banking relationship with the Applicants on 30 days notice.

22. Because of outstanding proceedings in Alberta in which the Applicants sought an injunction against Scotiabank, the Applicants' accounts were not closed until September, 2005 when the Alberta Court of Queen's Bench dismissed the Applicants' injunction motion.

23. As a result of the investigations undertaken in 2005, Scotiabank's decision to terminate related solely to the manner in which the Applicants were conducting their business as discussed in the preceding paragraphs.

24. Scotiabank categorically denies that its decision to terminate the Applicants' banking services was intended to eliminate GPAY as a competitor of Interac Online as alleged in paragraph 31 of the Amended Notice of Application.

25. Scotiabank denies that there has been a refusal to supply a product within the meaning of section 75 of the *Competition Act*. Rather, Scotiabank submits that termination of the Applicants' accounts was based solely on legitimate business, regulatory and legal concerns, and wholly unrelated to any matters relating to competition.

II. THE FACTS

(a) The Opening of Accounts by the Applicants

26. In August 1999, Raymond Grace approached the Scotiabank branch located in Sherwood Park, Alberta to establish a small business banking relationship with respect to his company B-Filer Inc., carrying on business as GPay. In the Application for Business Banking Services signed by Mr.

Grace dated August 6, 1999, he described GPay as a “financial collection” business, with annual sales/revenue of \$240,000 per year. The company was identified as having three employees.

27. After opening the single account for GPay in August 1999, no further accounts were opened until April 2004. Between April 2004 and March, 2005, Mr. Grace caused 108 accounts to be opened in the name of GPay, NPay, and B-Filer.

28. Most of the bank accounts were opened by Mr. Grace through utilization of Scotiabank’s telephone banking system during a two week period in February and March 2005, after the small business manager at the branch told Mr. Grace that his business exceeded the small business criteria and that no further accounts could be opened at the branch for the Applicants.

29. Whenever someone opens an account through telephone banking, the customer is asked: “Will this account be used to conduct business by, or on behalf of, someone other than the named account holder(s)?” Mr. Grace answered these questions in the negative. Scotiabank now knows that these answers were untrue, as described more fully below.

30. The opening of accounts by the Applicants violates Scotiabank policies in a number of respects.

31. It is Scotiabank policy that a single small business owner shall be granted only one primary profile at the Bank regardless of how many corporations he has incorporated to run the same business. The \$35 million in anticipated deposits for the 12 months beginning June 1, 2005 far exceed the usual trade terms for small business accounts.

32. Mr. Grace never disclosed to Scotiabank that the true and dominant business of the Applicants is to facilitate on-line gambling transactions with off-shore Internet casinos by Canadians wishing to place bets on-line with off-shore internet casinos. As a matter of policy, Scotiabank does

not knowingly permit its accounts to be used for purposes which Scotiabank considers to be illegal or which expose Scotiabank to unacceptable regulatory or reputational risk.

(b) Applicants' Operation Causes Bank Customers to Breach their Agreement with the Bank and Exposes Customers to Fraud

33. One of Scotiabank's paramount obligations is the maintenance of a secure banking system that minimizes the risk of fraud and maintains confidentiality of customer information. High security standards are essential in order to maintain the integrity of the Canadian banking system. Any process which undermines security for Canada's banking customers, undermines the integrity of the Canadian banking system.

34. To require Canadian banking customers to divulge their confidential Internet banking password to UseMyBank, and to allow NPay and GPay to enter into customers' secure Internet banking sites and undertake and perform account transactions as if they were the customer, undermines the security of the customer's account not only with respect to Scotiabank, but with respect to all Banks whose customers are using these services.

35. The Cardholder Agreement between Scotiabank and its customers prohibits customers from disclosing their PINs and passwords. By requiring bank customers to divulge their confidential bankcard numbers and on-line banking passwords, the Applicants are inducing breach of contract between Scotiabank and its banking customers. They are exposing Scotiabank's customers to the possibility of fraud.

36. The Applicants allege that they act as legal agents of Scotiabank customers. Scotiabank is required to know who is conducting transactions through each customer's account. Individuals or entities who have been granted a valid and legally binding Power of Attorney, which has been reviewed and approved by Scotiabank, must meet Scotiabank's "know your customer" guidelines. The person holding the Power of Attorney is able to access the grantor's account(s) by way of a

ScotiaCard and a electronic signature assigned to the Attorney. The Attorney may not use the grantor's card and electronic signature.

(c) GPay Cannot meet Scotiabank's "Usual Trade Terms" with respect to Business Accounts

(i) EMTs

37. Contrary to the Applicants' allegations at paragraph 15.10 of the Amended Notice of Application, the Applicants were and remain unable to meet Scotiabanks' usual trade terms for the provision of the services sought in this Application.

38. Mr. Grace is operating his companies using Scotiabank small businesses accounts in a manner which is contrary to Scotiabank policies for businesses which have grown as large as the Applicants'. In particular, electronic banking for business is designed for small business customers with low transaction and deposit volumes, whose annual sales do not exceed \$5 million. The total permitted deposit volume for small business accounts is \$400,000 per month, or a maximum of \$5 million per year.

39. According to the Applicants, only Scotiabank and the Royal Bank permit e-mail transfer for small business customers. Both banks impose maximum deposit limits on EMTs for business customers.

40. The Applicants' volume of business takes them well-beyond Scotiabank's criteria for qualification as a small business. If the Applicants were to qualify at all, it would have to be as a commercial banking customer of Scotiabank. None of the banks, including Scotiabank and Royal Bank, permit commercial banking customers to deposit EMTs into their commercial banking accounts. This is a necessary business decision made because of the enhanced risks associated with dealing with the larger volumes and numbers of transactions associated with commercial (rather than small business) banking customers.

41. Because of the manner in which the Applicants conduct their business, as fully realized during the investigations undertaken in early 2005, the Applicants would never have qualified as commercial banking customers of Scotiabank. Businesses applying for commercial banking status at Scotiabank are subjected to rigorous due diligence. The Applicants would have been classified as a “restricted business” because of the manner in which they conduct business (including the fact that they act as transferors of money), and their application for commercial banking services would have been denied.

42. Businesses that qualify as “small businesses”, as defined above, are permitted to accept email money transfers into their Scotiabank accounts. Small businesses can only accept a maximum of \$300,000 in email money transfer deposits per month. This limit is set by Certapay, a division of Acxsys Corporation, to reduce the possibility of fraud. Hence, the e-mail money transfers into the Applicants’ Scotiabank accounts were limited to a total monthly annual maximum of \$300,000. Based on the Applicants’ growth, their anticipated EMT transfers into their Scotiabank accounts far exceeds the \$300,000.00 monthly limits set by Acxsys Corporation.

43. Mr. Grace asserts that he deposited almost \$10 million in his Scotiabank accounts between June 1, 2004 and May 31, 2005. He also asserts that there will be a 341% increase in the volume of deposits in the next 12 month period. This amounts to an anticipated flow of funds through the Scotiabank accounts of almost \$35 million.

44. Mr. Grace admits that he is running a single business enterprise under the names of GPay, B-Filer, and NPay. Customers cannot circumvent the Small Business Banking Terms by using multiple corporations that in reality are engaged in the same business.

45. As admitted by the Applicants at paragraph 8.14 of the Amended Notice of Application, GPAY’s volume significantly exceeds the deposit limits described above.

(ii) Bill Payment System

46. Scotiabank's Bill Payment system is intended to facilitate the ease with which Scotiabank customers can pay invoices rendered, by companies that have provided goods or services to the public. The Applicants are not selling a good or service, but are acting as a conduit for money which is transferred from customers' accounts to the Applicants' accounts, with the end recipient almost always being an on-line casino or its management company.

47. As admitted in paragraphs 8.21 and 8.22 of the Amended Notice of Application, well before Scotiabank terminated GPay's biller services, each of the Canadian Imperial Bank of Commerce ("CIBC") the Toronto Dominion Bank ("TD"), and the Alberta Treasury Branches stopped providing GPay with biller services in 2003 because of security concerns about the manner in which the Applicants conduct their business.

48. As a result of the termination by CIBC, TD, and Alberta Treasury, the Applicants complained to the Competition Bureau and alleged a breach of Sections 75 and 79 of the *Competition Act*. The Bureau investigated and determined that there was no refusal to deal on the part of any of these banks. Instead, the Bureau concluded that each of the banks had legitimate business reasons for terminating GPay's biller services.

49. The Applicants' inability to obtain the products claimed in these proceedings, namely, Bill Payment services and EMTs, is not due to lack of competition as alleged in paragraph 8.2 of the Amended Notice of Application. Rather, it is due to the nature of the Applicants' business (i.e., the provision of services to customers engaging in illegal gambling that require disclosure of banking customers' passwords) and the violation of many valid and legitimate policies of Scotiabank.

(d) Applicants are in Breach of The Canadian Payments Association Rules for Clearing and Settlement

50. Scotiabank is prohibited by the Rules of the Canadian Payments Association (the “CPA”) from clearing transactions in which the customer’s authentication information is disclosed to third parties during an electronic transfer of funds. This is the case for all of the transactions processed by the Applicants.

51. The process through which Schedule I Banks and other CPA members exchange payment items, whether in paper or by electronic means, is referred to as “clearing”. Flows of value in one direction are netted against flows of value in the opposite direction. The financial institutions involved, including Scotiabank, “settle” the net amounts through their accounts at the Bank of Canada. The process of Clearing and Settlement is central to the operation of the national payments system. The Automated Clearing Settlement System (“ACSS”) is a system through which the vast majority of payment items in Canada – more than 17 million on an average day – are cleared.

52. On February 3, 2005 a new CPA Rule to support the clearing and settlement of on-line payments came into effect, namely, Rule E2.

53. Rule E2 sets out the requirements for the Exchange, Clearing and Settlement of on-line, electronic payment items. Scotiabank is bound by the CPA Rules, including Rule E2, with respect to the clearing and settlement of on-line payments. Section 5(a) of Rule E2 states:

In all matters relating to the Exchange, Clearing and Settlement of On-line Payment Items for the purpose of Clearing and Settlement each Member [which includes the Bank of Nova Scotia] shall respect the privacy and confidentiality of the payor [banking customer] and the payee [GPay, NPay Inc. and/or B-Filer Inc.] personal and financial information in accordance with applicable Canadian provincial and federal legislation ... In particular, only that information or data that is necessary to effect the processing of the On-line Payment Items is to be made available to the Acquirer and/or the Payee [NPay, GPay, NPay Inc. and/or B-Filer Inc.] during a

session. For greater clarity, the Payors' [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 during the On-line Payment Transaction Session. [emphasis added]

54. The Applicants are acting as an "Acquirer", as defined in Rule E2 of the CPA Rules. An Acquirer is defined as:

A person who captures transaction data from the Payee for transmittal to the Acquirer [financial institution] to reconcile the credit payment instruction sent by the Payors' [financial institution] to the Acquirer [financial institution].

55. Pursuant to Rule 5(b) of Rule E2, each financial institution that is settling amounts for non-CPA members must obtain a written undertaking from each non-CPA member to be bound by and adhere to the requirements of Rule E2. Moreover, Scotiabank, as the member financial institution, is responsible and liable for every on-line payment item and must indemnify the other financial institutions for any loss incurred by virtue of the clearing and settlement process.

56. The Applicants' manner of doing business, which is premised on the customer disclosing his or her confidential on-line banking password, is in contravention of Rule E2. The Applicants are unable to comply with Rule E2 because their business model is premised on the receipt of password information from banking customers who use their service. By requiring banking customers to divulge their confidential password information, it is not the banking customer that is "authenticating" him or herself by entering the website and using his/her secret password. Instead, it is GPay and/or NPay that purports to be "authenticating" the transaction.

57. The CPA Rules require that the customer authenticate him or herself during an on-line transaction, and not a third party such as the Applicants. By reason of CPA Rule E2, transfers of money into the Applicants' Scotiabank accounts are not eligible for clearing where the customer's confidential on-line banking passwords have been used by the Applicants to effect the transaction.

(e) Applicants' Business Raises Serious Regulatory and Reputational Risks

58. Off-shore Internet gambling is very likely illegal in Canada. It is almost certainly illegal for a Canadian resident located in Canada to place a bet with an on-line off-shore Internet gambling provider. Off-shore Internet gambling is known to be associated with other illegal activities including drug trafficking and money laundering.

59. The federal Parliament's power to enact criminal law in Canada has resulted in criminal sanctions for a broad range of gambling activities. Pursuant to section 197(1) of the *Criminal Code*, "bet" is defined to mean:

"a bet that is placed on any contingency or event that is to take place in or out of Canada, and without restricting the generality of the foregoing, including a bet that is placed on any contingency ... that is to take place in or out of Canada." [emphasis added].

60. Pursuant to section 202(1) of the *Criminal Code*, everyone commits an offence who:

- (a) *uses or knowingly allows a place under his control to be used for the purpose of recording or registering bets ...;*
- (b) *imports, makes, buys, sells, rents, leases, hires or keeps, exhibits, employs or knowingly allows to be kept, exhibited or employed in any place under his control any device or apparatus for the purpose of recording or registering bets ... or any machine or device for gambling or betting;*
- (c) *has under his control any money or other property relating to a transaction that is an offence under this section;*
- (d) *records or registers bets ...;*
- (e) *engages in ... the business or occupation of betting, or makes any agreement for the purchase or sale of betting or gaming privileges, or for the purchase or sale of information that is intended to assist in ... betting;*
- (f) *prints, provides or offers to print or provide information intended for use in connection with ... betting upon any horse-race, fight, game or sport, whether or not it takes place in or outside of Canada or has or has not taken place;*
- (g) *imports or brings into Canada any information or writing that is intended or is likely to promote or be of use in gambling ...*
- (h) *...*
- (i) *willfully and knowingly sends, transmits, delivers or receives any message by radio, telegraph, telephone, mail or express that conveys any information relating*

*to ... betting or wagering or that is intended to assist in ... betting or wagering;
or*

(j) *aids or assists in any manner in anything that is an offence under this section.*

61. Pursuant to section 202(2) of the *Criminal Code*:

“Everyone who commits an offence under this section is guilty of an indictable offence and liable:

*for a first offence, to imprisonment for not more than two years;
for a second offence, to imprisonment for a term not more than two
years and not less than fourteen days; and
for each subsequent offence, to imprisonment for not more than
two years ...*

62. In addition to the foregoing, sections of the *Criminal Code* specifically relating to gambling, section 21 of the *Criminal Code* is a provision of general application which is also relevant:

“(21)(1) Everyone is a party to an offence who

(a) *actually commits it;*

(b) *does or omits to do anything for the purpose of aiding any person to commit it;
or*

(c) *abets any person in committing it.*

(2) *Where two or more persons form an intention in common to carry out an unlawful purpose and to assist each other therein and any one of them, in carrying out the common purpose, commits an offence, each of them who knew or ought to have known that the commission of the offence would be a probable consequence of carrying out the common purpose is a party to that offence.*

63. The vast majority (approximately 98 percent) of the Applicants’ business involves money transfers to Internet off-shore casinos (or their management companies) from the bank accounts of Canadian citizens. UseMyBank, and its affiliated entity GPay, are the entities that “authenticate” the e-mail money transfer by entering directly into the customer’s Internet banking site, removing funds from the customer’s account, and ultimately funding Internet gambling.

64. There is a very strong argument that a Canadian citizen located in Canada who places a bet with an off-shore Internet gambler is committing a criminal offence. In particular, the Canadian located in Canada who is placing a bet with off-shore Internet casinos is most likely in breach of:

- (a) section 202(1)(a), because bets are recorded and registered on the internet gambler's computer by both the gambler and by the operator;
- (b) section 202(1)(b), because the internet gambler employs a device (his or her computer) for recording or registering bets;
- (c) section 202(1)(e), because the internet gambler makes an agreement for the purpose of betting or gaming privileges with the gambling operator and purchases information intended to assist in betting;
- (d) section 202(1)(g), because the internet gambler imports or brings into Canada by means of the internet, information that is intended to be used in gambling; and
- (e) section 202(1)(i), because the internet gambler sends messages that convey information relating to betting, provided that the word "telephone" in that section encompasses an internet computer link.

65. Pursuant to section 202(1)(c) of the *Criminal Code*, it is an offence to have under one's control any money relating to a transaction that is an offence under section 202. There is a very strong argument that the Applicants, in conjunction with their joint venture partner UseMyBank, by effecting transfers of money from Canadian customers' bank accounts to the Applicants' Scotiabank accounts, and ultimately transferring the money to off-shore Internet casinos (or their management companies), are very likely committing an offence pursuant to Section 202(1)(c).

66. There is also a very strong argument that the Applicants are in violation of section 21 of the *Criminal Code* by aiding and abetting the Internet gambler to commit these offences. In particular,

facilitating the transfer of funds from the Internet gambler's account to the Applicants' bank accounts at Scotiabank, and ultimately out to the Internet casinos, whether or not this occurs through a series of other intermediaries, likely constitutes aiding and abetting the Canadian banking customer in committing an offence.

67. The manner in which the Applicants conduct their business gives rise to the following concerns on the part of Scotiabank:

- (a) Money Services Businesses, including the Applicants, are not required to be licensed or registered with the government in any way. While the Applicants are required to comply with Canada's *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*, and its Regulations, it is very difficult for Scotiabank to be satisfied that the Applicants, with their enormous volume of transfers and in excess of 20,000 customers, are compliant.
- (b) Money Services Businesses have become an attractive means for money launderers or terrorists to move money outside the traditional financial services industry. They represent a high risk for Banks and are difficult to monitor effectively.
- (c) Money Services Businesses, particularly those that concentrate on Internet payments, are often used to maintain anonymity for individuals who are purchasing illegal or questionable goods or services over the Internet.
- (d) Scotiabank would be exposed to significant regulatory and reputational risk if it were determined that it was facilitating money laundering or terrorist financing or facilitating illegal activity by enabling the movement of money via the Applicants' business.

- (e) Money Services Businesses therefore require enhanced due diligence and monitoring by financial institutions. Scotiabank's extensive review of the Applicants' business practices revealed an unacceptable level of risk associated with continuing to do business with the Applicants.
- (f) **Scotiabank's Notice to Terminate its Banking Relationship with the Applicants**

68. As a result of Scotiabank's investigations begun in early 2005, Scotiabank advised the Applicants by letters dated May 11, 2005 that it would be terminating its banking relationship with them.

69. The Business Banking Services Agreement gives Scotiabank the right to terminate any banking service with its customer on 30 days' notice, for any reason. The Agreement provides further that banking services may be cancelled immediately, without notice, if a business customer defaults on any obligation to Scotiabank, including, *inter alia*, compliance with specific security procedures and Scotiabank's verification and authorization requirements. Scotiabank chose not to rely on the section of the Agreement permitting immediate termination, because to do so would have required Scotiabank to divulge the reasons for terminating the relationship "with cause". Scotiabank elected not to rely on the "with cause" section of the Agreement so as to maintain confidentiality over its fraud detection system and the specifics of the investigation.

70. The Bill Payment Agreement with GPay also allows Scotiabank to terminate GPay's status as a bill payee on 30 days' notice, without reason.

- (g) **The Termination of the Agreements with the Applicants was Unrelated to Interac Online**

71. Contrary to the Applicants' (unfounded and unsupported) assertion, the termination of the agreements with the Applicants had nothing to do with the establishment of Interac Online. Rather,

it was based solely on the regulatory, reputational, legal, and policy concerns and breaches revealed by the comprehensive investigation undertaken by Scotiabank in early 2005.

72. The vast majority of transactions (approximately 98% by volume) processed by the Applicants are payments to off-shore Internet gambling casinos or their management companies. Interac Online will not allow its facilities to be used for this purpose. The Applicants' business is not in competition with that of Interac Online.

73. Interac is a national organization linking enterprises that have proprietary networks. This allows the enterprises to communicate with each other for the purposes of exchanging electronic financial transactions. Any company incorporated in Canada is eligible to join Interac, so long as it complies with Interac's rules and regulations.

74. Security of the Interac system is fundamental to maintaining its integrity. Historically, Interac operated through the use of the customer's confidential PIN. This is similar to the customer's Internet banking password which customers use when performing transactions via the Internet using their Bank's website. The PIN and the Internet banking password are known as the customer's "electronic signature".

75. Scotiabank, along with Bank of Montreal, Royal Bank, CIBC and TD Canada Trust, have recently begun to offer Interac Online. Interac Online is a payment option that allows banking customers to pay for goods and services on the Internet by debit directly from the banking customers' bank accounts, using Internet banking. As of June 2006, approximately 20 merchants offer Interac Online as a payment option for goods or services offered by those merchants.

76. When the banking customer is on a merchant's website that offers Interac Online as a payment option, the banking customer can choose Interac Online as the payment method. The

merchant website would then redirect the banking customer to the Interac webpage. There, the banking customer would select his or her financial institution.

77. The banking customer is then directed to his or her financial institution's website. The banking customer then logs in directly to the bank's secure website, selects the account that he or she wants to pay from, and confirms payment. Thereafter, the banking customer is redirected back to the merchant's website for the confirmation page.

78. When a customer is accessing Interac Online, it is the customer that "authenticates" the transaction by using his or her own PIN or password. The customer is never required to divulge his or her "electronic signature" to a third party. Personal authentication by the customer is essential in order for the banks to clear and settle the accounts between them pursuant to CPA Rule E2.

79. Interac Online payments are cleared and settled through the usual ACSS clearing and settlement system.

80. The fundamental differences between Interac Online and the Applicants' business are that:

- (a) there is no disclosure of confidential customer information to third parties when using the Interac system.
- (b) Interac Online cannot be used to fund on-line gambling.
- (c) Interac Online facilitates the purchases of goods or services. The vast majority of the Applicants' business does not facilitate the purchase of goods or services. Instead, the Applicants are acting as a Money Services Business and are simply acting as a conduit to transfer money anonymously between banking customers and internet casinos or their management companies to allow banking customers to gamble on-line.

III. SUBMISSIONS

(a) **Relevant Product Market**

(i) **Biller Services**

81. Scotiabank denies that “Scotiabank Biller Services” is a separate product market for the purposes of this Application. Rather, the relevant product market is at least as broad as the “Biller Services” of the five major chartered banks (it also includes the Biller Services of Alberta Treasury Branches and the Fédération des caisses Desjardins du Québec) and, in addition, includes EMT payments.

82. As admitted by the Applicants in the Amended Notice of Application, the Applicants’ business model requires that they have access to customers of the five major chartered Banks who make use of online banking facilities with a bank card. The Applicants are indifferent as to which banks such customers are clients. Therefore, each of the five chartered Banks (as well as Alberta Treasury Branches and the Fédération des caisses Desjardins du Québec) is capable of supplying the product required by GPAY to operate its business.

83. At paragraphs 8.16 and 8.17 of the Amended Notice of Application, the Applicants admit that any bank can provide the service required for the Applicant’s business. The appropriate product market is therefore the services provided by all financial institutions that allow customers to transfer funds electronically to a third party. That is, Biller Services plus EMT.

84. The fact that the Applicants have brought an Application against only Scotiabank does not allow it to unduly restrict the definition of the relevant product market. The Applicants theoretically could have brought a proceeding against each Bank that has terminated their Biller Services, namely, Alberta Treasury, CIBC and TD.

(ii) EMT Business Deposit Accounts are Substitute Products for Biller Services

85. Scotiabank submits that EMT Business Deposit Accounts are adequate substitutes for Biller Services. At paragraph 8.22 of the Amended Notice of Application, the Applicants admit that in December 2003, CIBC, TD and Alberta Treasury Branches terminated GPAY as a bill payee and “as a result, GPAY began relying on EMTs to process payments from CIBC and TD”. Hence, the Applicants were able to replace Biller Services at CIBC, TD, and Alberta Treasury with EMTs. The growth in the Applicants’ business after December 2003 demonstrates that EMTs are an acceptable substitute for Biller Services.

86. EMTs are clearly a substitute for Biller Services as demonstrated by the exponential growth in the number of EMTs processed by the Applicants since December 2003 when CIBC, TD, and Alberta Treasury terminated the Applicants as Billers on their Bill Payment system.

87. Since Scotiabank terminated the Applicants as Billers on the Scotiabank Bill Payment system in September 2005, the Applicants have not had to turn away a single customer wishing to transfer funds using the Applicants’ services. The Applicants have found ways to manage the increased volume of EMTs, with the result that their business has continued to grow.

(iii) EMT Business Deposit Accounts are not a Relevant Product Market

88. Scotiabank submits that EMT Business Deposit Accounts are not a relevant product market but rather are part of the Biller Services and EMT payments product market.

89. As noted above, EMT Business Deposit Accounts are substitutes for Biller Services. As well, EMT payments can and are being made into personal accounts as well as business accounts and those accounts also form part of the relevant market.

(b) The Relevant Market

90. The Applicants allege that the relevant market for the purposes of this Application is the market for online bank card debit payment processing. In fact, the overwhelming majority of the Applicants' business consists of facilitating transfers to off-shore Internet casinos. Scotiabank submits that the relevant market for the purpose of the Application is the market for payment processing to off-shore Internet casinos.

91. While the Applicants have been operating their business since December 2002, they have not been able to sign up any Canadian retail merchants of consequence. The Applicants' service is not attractive to mainstream Canadian merchants. The Applicants' business is confined to facilitating payments to off-shore Internet casinos, or other businesses that cater to individuals wishing to maintain a high degree of anonymity, such as dating agencies that cater to married people seeking discreet intimate encounters.

92. Neither Scotiabank nor Interac Online participates in, nor wishes to participate, either directly or indirectly, in the market to facilitate payments to off-shore Internet casinos.

(c) Section 75 Criteria

93. The Applicants are not entitled to a remedy under s.75 because they cannot establish the following criteria:

(i) Substantially Affected in the Business (s.75(1)(a))

94. Since the termination of the Applicants' agreements with Scotiabank, the Applicants have continued in business and have replaced Scotiabank's services with services from the Bank of Montreal, Royal Bank and the Caisse Populaire Desjardins.

95. The Applicants have increased the volume of transactions processed since Scotiabank terminated the banking relationship in September 2005. Scotiabank submits that the Applicants

have not been substantially affected in their business as a result of the refusal by Scotiabank to provide the Applicants with banking services.

(ii) Insufficient Competition Among Suppliers in the Market (s.75(1)(b))

96. The refusal to deal was not “because of” insufficient competition among suppliers of a product. Rather, the refusal to deal was because of legitimate business and reputational, policy, and legal concerns of Scotiabank. Competitive concerns were completely irrelevant to and did not form any part of Scotiabank’s decision to terminate its services to the Applicants.

(iii) The Applicants are not willing or able meet Usual Trade Terms (s.75(1)(c))

97. The Applicants cannot meet Scotiabank’s usual trade terms including:

- (a) Scotiabank will not supply bank services to businesses which are involved in activities which are most likely illegal, in this case, gambling by Canadian residents at off-shore Internet casinos.
- (b) Scotiabank will not supply bank services to businesses which require Scotiabank customers to disclose their confidential authentication information (i.e. Internet passwords) to third parties, thus exposing Scotiabank and its customers to risk of fraud and causing the customers to violate their Cardholder Agreements.
- (c) The Applicants are not entitled to accounts and services which are only available to small business customers. The Applicants are not a small business.
- (d) The Applicants made misrepresentations to Scotiabank as to the nature of their business. Had the Applicants truthfully and accurately described the complete nature and manner of conducting their business at the outset, their accounts would not have been opened. Scotiabank will not provide its services to a business such

as the Applicants' because of legitimate business, reputational, policy, and legal concerns.

- (e) Compliance with Rule E2 of the CPA prohibits Scotiabank from clearing and settling EMT transfers into the Applicants' accounts, because the Applicants' business model requires the disclosure of the customer's confidential authentication information to a third party.

(iv) No Adverse Effect on Competition in the Market (s.75(1)(e))

98. Scotiabank denies that its refusal to provide bank accounts to the Applicants will have an adverse effect on any market in Canada.

99. As stated elsewhere, the vast majority of the Applicants' business is the processing of money transfers to off-shore Internet casinos. Accordingly, the only business affected is gambling by Canadians at off-shore Internet casinos, which is most likely illegal, and, in any event, for which there are alternative means of funding.

100. Neither Scotiabank nor Interac Online engages in the business of processing money transfers to off-shore Internet casinos. Neither Scotiabank nor Interact Online competes with the Applicants.

(d) Business Justification Defence

101. Scotiabank submits that it is entitled to rely on the "business justification defence" in regard to its decision to refuse to supply the Applicants with banking services.

102. The "business justification defence" was first alluded to and articulated in the case The Director of Investigation and Research and Xerox Canada Inc. CT-89/4. Madame Justice Reed

made the following statement at p.64:

“Another hypothetical situation was whether section 76 could catch a manufacturer who refused to supply certain customers merely because he wished to change his distribution system for the product. Again, in the absence of an actual fact situation, it is impossible to conclusively answer such a question. At the same time, one can question whether an inability to obtain supply in such circumstances would necessarily meet the test of occurring “because of insufficient competition among suppliers of the product.” It may very well be that the inability to obtain supply in such circumstances could be related to a legitimate business decision unconnected to anti-competitive factors.” [emphasis added]

103. Scotiabank submits that s.75 of the *Competition Act* was not designed to preclude a person from refusing supply of a product to another person in circumstances where such refusal arose solely from legitimate business purposes. Rather, s.75 was designed to provide a remedy only in circumstances where the refusal related to matters pertaining to competition. This is made clear by s.75(1)(b) and (e) of the Act wherein a remedy is only available where the refusal was “because of insufficient competition among suppliers of the product” and “the refusal to deal is having or is likely to have an adverse effect on competition in a market”.

104. As stated throughout this Response, Scotiabank’s refusal to supply banking services to the Applicants was based solely on legitimate business, reputational, regulatory and legal concerns which arose out of an investigation into the manner in which and the purpose for which the Applicants carried on business and had nothing to do with any matters relating to competition. Accordingly, Scotiabank submits that the business justification defence applies to preclude any remedy under section 75 of the *Competition Act*.

IV. CONCLUSION

105. Scotiabank terminated its agreements with the Applicants for legitimate and well-founded business, reputational, regulatory and legal reasons based on the manner in which and the purpose for which the Applicants’ business is conducted.

106. The termination was a result of investigations which fully disclosed the true nature of the Applicants' business and had nothing to do with competition or competitive concerns.

107. These investigations revealed that the Applicants' business is a Money Services Business involved primarily in the transfer of money to off-shore internet gambling casinos. Gambling by Canadians at off-shore on-line casinos is most likely illegal. The Applicants were likely facilitating illegal activity using Scotiabank's accounts, while they remained open. Because of the nature of the business and the manner in which the Applicants carry on their business, Scotiabank was exposed to significant legal, regulatory and reputational risk if it continued to provide the Applicants' with banking services.

108. The Applicants' are not entitled to a remedy since they cannot establish the criteria necessary to succeed under section 75 of the *Competition Act*.

109. Therefore, Scotiabank requests that this Application be dismissed with costs.

110. Scotiabank has no objection to the proceedings being conducted in English or to the electronic filing of documents.

Dated: June 22, 2006

McCarthy Tétrault LLP
Suite 4700,
Toronto Dominion Bank Tower
Toronto, ON M5K 1E6

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

Glen G. MacArthur LSUC# 13669A
Tel: (416) 601-7888

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

Solicitors for the Respondent, The Bank of Nova Scotia

B-FILER INC.
Applicants

and

THE BANK OF NOVA SCOTIA
Respondent

Court File No: CT 2005-006

COMPETITION TRIBUNAL

RESPONSE TO AMENDED NOTICE OF APPLICATION
PURSUANT TO SECTION 75 OF THE COMPETITION ACT

McCarthy Tétrault LLP
Suite 4700
Toronto Dominion Bank Tower
Toronto ON M5K 1E6

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

Glen G. MacArthur LSUC #: 13669A
Tel: (416) 601-7888
Fax: (416) 868-0673

Lisa M. Constantine LSUC#: 35064B
Tel: (416) 601-7652
Fax: (416) 868-0673
Solicitors for the Respondent
4094408v6