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 CHRISTOPHER MATHERS
(Sworn November 23, 2005)

I, **CHRISTOPHER MATHERS**, of the City Of Toronto, in the Province of Ontario,

MAKE OATH AND SAY:

Professional Qualifications and Experience

1. I have lectured and provided training in anti-money laundering ("AML") to both private and public sector organizations in more than 15 countries. I have provided advice and assistance on money laundering compliance and organized criminal activities to various foreign public sector organizations, including the Canadian Bar Association, the Investment Dealers

Association, the Ontario Securities Commission, the Toronto Stock Exchange, as well as advice to numerous foreign jurisdictions.

2. For 20 years, between 1975 and 1995, I was a member of the Royal Canadian Mounted Police (the RCMP). During most of my career with the RCMP, I worked undercover with the RCMP, and also with the U.S. Drug Enforcement Administration and the U.S. Customs Service. I was a senior undercover operator with the RCMP Proceeds of Crime Section, where I established and operated a number of "store front" money laundering businesses in Canada and the U.S., targeting Columbian, Russian and Asian organized crime groups.

3. I retired from the RCMP in 1995 and joined the Forensic Division of the International accounting firm KPMG. In 1999, I was appointed to the position of President of KPMG Corporate Intelligence Inc. I was responsible for international due diligence, asset recovery operations, and the investigation and prevention of organized crime and money laundering. I reported directly to the Chairman of KPMG. In this position, I provided advice to corporations, governments and individuals in the areas of foreign due diligence and threat assessment, corruption, money laundering compliance, fraud prevention and foreign and domestic information gathering.

4. I have written extensively on issues relating to money laundering. I also authored a non-fiction book in 2004 entitled "*Crime School: Money Laundering*" which has been published in both the United States and Canada and will be published in China and Estonia in 2006.

5. I have been qualified as an expert witness in money laundering in the Ontario Provincial Superior Courts.

6. Attached hereto and marked as Exhibit **"A"** is a copy of my Curriculum Vitae.

Material Reviewed

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

(a) Notice of Application for Leave pursuant to Section 103.1 of the *Competition Act*;

(b) Notice of Application pursuant to Sections 75 and 77 of the *Competition Act*;

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

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

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

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) Representations of the Bank of Nova Scotia in response to the Application for Leave, pursuant to Section 103.1 of the *Competition Act*;

8. In addition to the foregoing, I was also provided with the Decision of the Honourable Mr. Justice Lefsrud, dated September 22, 2005 with respect to the Motion by the Applicants for an Injunction in the Alberta Civil Court.

Brief Overview of the Facts

9. Based on my review of the above-noted documentation, I believe that the following is a brief summary of the facts that are relevant to my opinion on the issues that I have been asked to consider. The source of my information and belief with respect to the following factual issues is derived from the materials reviewed.

10. The Applicants, together with UseMyBank, operate a joint venture business enterprise which facilitates the transfer of money from banking customers accounts to third parties.

11. If a banking customer wishes to transfer money to a third party through the services of the Applicants and UseMyBank, the banking customer would click on the UseMyBank icon. The banking customer would be prompted to provide the banking customer's bank card and internet password. The Applicants and UseMyBank would take the customer's bank card number and password and would enter into the customer's bank account and effect a transfer of money from the customer's bank accounts to the Applicants' account at The Bank of Nova Scotia ("Scotiabank") by way of e-mail money transfer. The Applicants could also effect transfers of money from banking customers' accounts by entering into the banking customers' accounts and transferring money to GPay as a Scotiabank bill payee and these funds would later be released from Scotiabank's suspension accounts to the Applicants' accounts at Scotiabank.

12. Based on my review of the materials, it is clear that much of the Applicants' business involves transferring funds from Canadian banking customers' accounts to the Applicants'

Scotiabank accounts, and apparently ultimately out to off-shore internet casinos . The Applicants' service in conjunction with UseMyBank allows Canadian customers to place bets at off-shore internet casinos.

Overview of Money Laundering and Terrorist Financing Regulatory Regime in Canada

13. The Proceeds of Crime (Money Laundering) and Terrorist Financing Act (the "*PCMLTF*") is legislation to facilitate the combating of laundering proceeds of crime and financing terrorist activities. The purpose of the *PCMLFT* is described in section 3 of the Act as:

- to implement specific measures to detect and deter money laundering and the financing of terrorist activities to facilitate the investigation or prosecution of money laundering and terrorist financing offences, including:
    - establishing recordkeeping and client identification requirements for financial services providers and other persons that engage in businesses, professions or activities that are susceptible to being used for money laundering and the financing of terrorist activities, requiring the reporting of suspicious financial transactions and of the cross-border movements of currency and monetary instruments; and
    - establishing an agency that is responsible for dealing with reported and other information:
        - to respond to the threat posed by organized crime by providing law enforcement officials with the information they need to investigate and prosecute money laundering or terrorist financing offences, while ensuring that appropriate safeguards are put in place to protect the privacy of persons with respect to personal information about themselves; and,
        - to assist in fulfilling Canada's international commitment to participate in the fight against transnational crime, particularly money laundering and the fight against terrorist activities.

14. In the balance of this Affidavit, I provide my expert opinion with respect to whether the Applicants' business raises money laundering concerns. I will also consider whether providing

banking services to the Applicants would raise money laundering concerns for Scotiabank and whether a Schedule 1 bank such as Scotiabank should be providing banking services to the Applicants from the perspective of risk management in the context of money laundering issues.

Are the Applicants Operating a Money Services Business?

15. The PCMLTF defines a Money Services 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 those activities with a person or entity that is not an account holder.*

16. The Applicants, in conjunction with their joint venture partner UseMyBank, are operating a Money Services Business, as defined by the *PCMLTF*. The Applicants are engaged in the business of remitting funds and transmitting funds using email money transfer and by using the Bank's bill payment system.

Are The Applicants Conducting Business By Or On Behalf of Third Parties?

17. Whenever accounts are opened, financial institutions such as Scotiabank are required to undertake certain due diligence mandated by the *PCMLTF* and the Regulations thereunder. One such requirement is that the individual wishing to open a new account must be asked whether the accounts will be used by or on behalf of a third party.

18. I have had an opportunity to review the Affidavit of Robert Rosatelli sworn July 12, 2005. At Exhibit "M" to that Affidavit, there is a transcript of a telephone conversation between Raymond Grace, who had apparently contacted Scotiabank Telephone Banking in order to open up additional accounts for his business enterprise, and the Scotiabank Telephone Banking

representative. In accordance with Scotiabank's obligations under the legislation, the telephone banker asked:

> *And will this account be used to conduct business on behalf of someone other than the named account holder?*
>
> *Mr. Grace responded: "No."*

19. Based on my review of the material filed with the Competition Tribunal, this answer is false. The Applicants were using their Scotiabank accounts to conduct business on behalf of others, namely, other banking customers who instruct the Applicants to transfer money from their bank accounts to the Applicants' bank accounts. The Applicants are then responsible for remitting payment on behalf of the banking customer to others, including off-shore Internet casinos.

How Do Criminals Use Money Services Business Such as the Applicants' Business to Launder Money or Fund Terrorist Activities?

20. In order to avoid detection by law enforcement, persons involved in international criminal activities such as drug trafficking must inject their illegal profits into the electronic banking system through a process referred to as "Placement" or "Conversion".

21. The next stage in converting the money is known as "Layering" or "Concealment". This involves creating a series of financial transactions, or layers, to separate the proceeds from their illegal source.

22. The final stage is known as "Integration". This involves co-mingling illegal monies with more legitimate proceeds to create a perception of legitimacy.

23. In Canada, criminals have an additional obstacle to overcome. Since they normally deal in Canadian currency, they are obliged to convert their profits into foreign currencies, usually U.S. dollars, if they wish to fulfill their financial obligations to foreign suppliers.

24. Due to the monetary thresholds set by the legislation (in the case of a Bank such as Scotiabank, $10,000 and a Money Services Business such as the Applicants, $3,000), criminals will often move amounts of money that are below the thresholds for transaction reporting. By using smaller amounts per transaction, the criminal is required to conduct multiple concurrent transactions and make use of a variety of money laundering techniques.

25. The products and services of on-line gaming web sites that offer casino gaming and sports wagering can be and frequently are used by criminals to launder the proceeds of crime. The following scenario illustrates the method by which the Applicants' services can be subverted to launder the proceeds of crime through on-line gaming. By reason of my experience in these matters, I can attest that this scenario represents a shown and used method of laundering money.

26. Third-party payments, such as those facilitated by the Applicants, are a very common method by which criminal proceeds or terrorist financing payments are laundered. It is a simple way in which to transfer wealth from one jurisdiction to another. Money Services Businesses such as the Applicants are a magnet to organized crime groups as they represent a relatively easy means of laundering money.

(a) Money Laundering Scenario Using the Applicants' Services

27. Person A and Person B are members of the same drug trafficking organization. They both have bank accounts at Canadian financial institutions and they have been successfully

depositing cash into the electronic banking system through a variety of methods without detection.

28. Person A and Person B also have bank accounts in off-shore jurisdictions.

29. Person A and Person B register independently as "Buyers" with UseMyBank and also independently register as customers with two unrelated on-line gaming websites that provide wagering on sporting events. As Exhibits "D" and "E" to the Affidavit of Robert Rosatelli sworn July 11, 2005 demonstrate, the UseMyBank services for transferring money are available at hundreds of off-shore casinos, many of which offer the ability to place bets on the outcome of sporting events.

30. Through a series of debit transactions with UseMyBank, both Persons successfully transfer the Canadian dollar equivalent of U.S. $25,000 into their respective accounts at the on-line sports books. For calculation purposes in the example that follows, a flat fee of $50 is applied to each winning wager.

Person A makes the following wagers on games played in the National Football League at Sports Book #1:	Person B makes the following wagers on games played in the National Football League at Sports Book #2:
Opening balance $25,000.	Opening balance $25,000.
Week 1 Miami v. Buffalo $2500 on Miami – Win Balance in account $29,950.	Week 1 Miami v. Buffalo $2500 on Buffalo – Lose Balance in account $22,500.
Week 2 Kansas City v. Denver $2000 on Kansas City - Win Balance in account $31,900.	Week 2 Kansas City v. Denver $2000 on Denver - Lose Balance in account $20,500
Week 3 Dallas v. Philadelphia $5000 on Philadelphia – Lose Balance in account $26,900.	Week 3 Dallas v. Philadelphia $5000 on Washington – Win Balance in account $25,450

Week 4 Green Bay v. Minnesota $10,000 on Green Bay – Lose Balance in account $16,900.	Week 4 Green Bay v. Minnesota $10,000 on Minnesota – Win Balance in account $35,400.
Week 5 Chicago v. Detroit $15,000 on Chicago – Lose Balance in account $1,900.	Week 5 Chicago v. Detroit $15,000 on Detroit – Win Balance in account $50,350

31. Person B requests a payout of U.S. $50,000 from Sports Book #2. The payout is provided in the form of a U.S. dollars cheque that is made out to Person B. Person B couriers the cheque from the Sports Book to his off-shore bank where it is deposited.

32. The cheque from the on-line casino/Sports Book, once deposited is returned to the on-line casino/Sports Book's bank in a foreign jurisdiction where it is unlikely to be traced by law enforcement.

33. Thus, using a series of opposing wagers, Person A and Person B have successfully transferred U.S. $50,000 in narcotic trafficking proceeds to an account in an off-shore jurisdiction. The only cost would be the fee deducted by the on-line casino/Sports Book. The location of the money is undetectable to domestic law enforcement since the money trail has been layered or concealed by the multiple smaller transactions between the originating bank, UseMyBank, the on-line Sports Book, and other intermediary financial institutions.

34. The same scenario could apply to certain poker products, such as Texan Hold'em if co-conspirators are able to contrive situations where they were only wagering against each other.

(b) How Can the Applicants' Service be used by Money Launderers or Terrorist Financers in Foreign Jurisdictions?

35. I am I am advised by Lynne Moran, legal counsel at Scotiabank and verily believe that the following is a real scenario that recently came to the attention of Scotiabank through Scotiabank's compliance officers in New York, as a result of monies received by way of an incoming telephone transfer from Beirut, Lebanon.

36. A Scotiabank customer residing in Ottawa used the services of the Applicants to transfer money from his Scotiabank account to fund an off-shore on-line casino gambling account. A review of the Ottawa Scotiabank customer's account indicates that money was transferred from the Ottawa customer's account to GPay's account at Scotiabank. On September 2, 2005, GPay alone made five transfers from the customer's account totaling $6,178.85

37. In October 2005, an inbound transfer in the amount of $10,000 in U.S. funds was received by Scotiabank's New York Agency for payment to the account of the Ottawa Scotiabank customer.

38. As part of Scotiabank's due diligence, the payment issued by the Lebanon bank came to the attention of Scotiabank's compliance officers located in New York. Upon investigating the matter, the compliance officers learned from the Ottawa Scotiabank customer that the money being forwarded to him was the proceeds of his winnings as a result of successful bets placed with the off-shore on-line casino, which had originally been funded through the services of the Applicants.

39. Lebanon is known to be a narcotics source country and also a potential source of terrorist financing. What is most troubling about the above-described transaction is that the payment

from the bank in Beirut, Lebanon appears to have been issued by a party that was completely unrelated to the initial transaction of placing the wager and funding the gambling account of the off-shore on-line casino.

40. The above-described transaction presents a clear risk for the Bank, in that money being issued by a bank in Beirut, Lebanon from a source which appears to have had nothing to do with the original transaction. The monies being transferred to the Ottawa customer could well represent the proceeds of crime or terrorist financing monies.

What Risk is Scotiabank Exposed to if They are Forced to Deal with a Money Services Business Such as the Applicants?

41. Financial Institutions typically rely on one another . It is generally understood that the correspondent financial institution is conducting appropriate due diligence and "know-your-customer" procedures on all of their customers.

42. By their very nature, Money Services Businesses are at a higher level of risk of exposure to money laundering activities. See for example the scenarios described in the preceding section.

43. When a bank allows its customers to conduct financial transactions over the Internet, those customers can only transact business with (i.e. send the funds to) entities that the bank can confidently say are *bona fide*. For a "payee" to be accepted as such, the payee must submit to a standard client acceptance procedure that is consistent with the know-your-customer requirement in the *PCMLTF*.

44. Without the know-your-customer requirement, the Bank has no way of knowing whether or not a payee is providing real goods and services. The client acceptance procedure assures the Bank that it is not acting as a conduit for the transfer of proceeds of crime from a customer who

may be involved in criminal activity. Allowing such transactions to take place would make the Bank an unwitting accomplice of money launderers.

45. Mr. Grace has asserted on behalf of the Applicants that the Applicants do not even know the goods or services that are being purchased by the banking customers that use their services to transfer funds. The Applicants' business model allows customers to transfer funds to unknown persons and/or corporations and, in particular, entities that have not been vetted by the Bank. This places the Bank in an untenable position. If the Bank allows such transactions to take place, it may be unknowingly allowing inappropriate or illegal transactions in violation of the *PCMLTF*.

46. Guideline 4 under the *POCMLTF* requires all financial entities, including banks and Money Services Business such as the Applicants to implement a compliance regime to comply with their reporting, record-keeping, and client identification requirements.

47. The Applicants are required to establish a compliance regime as defined in sections 3 and 4 of Guideline 4, and to subscribe to the four generally accepted tenets of money laundering compliance that form the backbone of any effective anti-money laundering program. These four tenets are:

(a) the appointment of a compliance officer;

(b) the development and application of compliance policies and procedures;

(c) independent testing and review of compliance policies and procedures to test their effectiveness; and

(d) an on-going compliance training program.

48. The Applicants are also bound by Guideline 6 of the *POCMLTF* that requires the Applicants to establish and maintain appropriate client and transaction records.

49. The Applicants' joint venture partner, UseMyBank, does not require disclosure of sufficient information from a person signing up to use their service to comply with the requirements under the *PCMLTF*, nor does it take any steps to verify the accuracy of the information provided by the seller. In particular, UseMyBank does not elicit sufficient information from the person signing up to use its service to be able to reliably state that the Seller is not a risk as a client. As a result, the Applicants and UseMyBank are at risk of unwittingly assisting money launderers in "Placement", "Layering", and "Integration" as described in the preceding section.

50. Moreover, because the Applicants and UseMyBank do not have sufficient safeguards in place, any Bank that provides banking services or is required to provide banking services to the Applicants is at risk of becoming an unwitting accomplice to money launderers. I can provide an actual example of how fundamentally inadequate the Applicants' and UseMyBank's system is for determining whether a customer of UseMyBank is a risk for money laundering.

51. On Saturday, November 19, 2005, at approximately 10:00 a.m., I logged on to the UseMyBank website using an assumed name of Au Porteur. I registered as a "Seller" on the UseMyBank site. I provided a contrived address of 24 Buada 6, Yaren, Yaren 66, Nauru. I provided a telephone number of 674-444-3181, which happens to be the telephone number of the Nauru Department of Economic Development.

52. The Financial Action Task Force (the "FATF") is an inter-governmental body, whose purpose is the development and promotion of policies, both at national and international levels, to combat money laundering and terrorist financing. The FATF is based in Paris, France, and has 33 member countries including the United States, the United Kingdom, Canada and Australia, among others.

53. A part of the FATF's mandate is to collect information and to identify non-co-operative countries with respect to money laundering. Nauru has been on the FATF list of non-co-operative countries and territories since the FATF's inception. Specifically, Nauru is known internationally as a money laundering centre, and is frequently used by money launderers. Any entity, including a Money Services Business that has undertaken proper due diligence with respect to its customers, should be extremely wary of any customer connected with Nauru.

54. UseMyBank requested me to provide further information such as company address and website, but I declined to do so.

55. On the Seller - Profile screen of UseMyBank's website, there are three methods of disbursement for a Seller to receive payment from UseMyBank:

(a) direct deposit into a Canadian bank account;

(b) wire transfer; or

(c) cheque.

56. Because I was using an assumed name that does not have a bank account, I selected the "cheque" option. UseMyBank advised me that my information had been updated. UseMyBank responded to my email address with the following message:

Cheque will be made payable to: Au Porteur.
Mailing address:
Au Porteur
24 Buada 6
Yaren, Yaren
66
Nauru

57. The assumed name that I adopted, "Au Porteur", which was accepted by UseMyBank, is the French translation of "To The Bearer". As a result, any cheque from UseMyBank made payable to this name would, in fact, create an anonymous bearer cheque that could be cashed anywhere in the world by anyone.

58. Attached to this Affidavit and marked as **Exhibit "B"** are copies of the screens from the above-noted session, as well as the email I received from UseMyBank at an email address auporteur@hotmail.com.

59. The foregoing is a very simple but also a very dramatic example of how easy it is to become registered with UseMyBank under an assumed name, which would allow me to receive cheques payable "To The Bearer", which could be cashed anywhere in the world by anyone.

60. Bearer instruments, such as cheques made "To The Bearer" or "Au Porteur" are of value to criminal and extremist groups because they are anonymous and easily transferable. They can be passed from one person to the next without the need for any intermediary transaction with a financial institution. The use of a bearer cheque eliminates the inherent problems associated with the physical movement of large amounts of currency. A cheque made payable to "To The Bearer" can be easily concealed in the mail and does not pose the same types of security/storage problems as currency.

61. Criminal and extremist groups typically do not make use of only one technique to launder their funds. To avoid detection they will make use of a variety of techniques simultaneously.

62. If the "Seller" registered as "Au Porteur" with UseMyBank was actually distributing an illegal commodity such as drugs or weapons, the purchaser of these commodities could make use of the Applicants' system to effect payments which would be anonymous. The Seller could purport to be providing any type of goods or services.

63. Here is an example of how a Scotiabank account could be used in the foregoing scenario. The "Purchasers" have already put their money through the "Placement" stage, by depositing it, probably in small quantities to avoid detection, in the Canadian banking system. They will have registered as "Purchasers" with UseMyBank.

64. Purchaser A in Canada wishes to purchase a prohibited item such as an automatic weapon from "Au Porteur" in Nauru, who is already registered as a "Seller" with UseMyBank. They agree upon a price of $5,000 (U.S. funds).

65. Purchaser A logs on to the UseMyBank website and provides his bank card password with instructions to the Applicants to remove $5,000 from his account and transfer it to the "Seller", Au Porteur.

66. The "Seller", Au Porteur, receives a cheque from UseMyBank for $5,000 (U.S. funds) less the necessary fees. Pursuant to the instructions already accepted by UseMyBank, the cheque is made payable to "Au Porteur" (i.e. To The Bearer). The "Seller" that had been registered with UseMyBank as Au Porteur receives the cheque from UseMyBank. He takes the cheque made payable to Au Porteur (i.e. To The Bearer) and gives the cheque to Extremist "Z" in Afghanistan

for originally supplying the weapons. The example could go on and on, as the cheque made payable to Au Porteur (To The Bearer) is passed from one person to the next. All of the transactions have been both illegal and anonymous, thanks to the system set in motion by UseMyBank and the Applicants.

67. The ease with which I was able to put in place a situation which would have allowed a money launderer or terrorist financer to receive cheques that could be cashed by anyone, anyone in the world, underscores the total inadequacy of the Applicants' system. The Applicant and its joint venture partner UseMyBank, do not meet the know-your-client requirements of the *PCMLTF*. Moreover, the Applicants are not in compliance with the U.S. *Patriot Act*, **[NTD: attach Act]**in that the Applicants are unable to confirm the true identity of the Seller. The system can be easily subverted. There is no provision for a face-to-face encounter, with the result that the Applicants are unable to examine a "Seller's identification" before UseMyBank confirms that they have been properly registered as a Seller, eligible to use its system and receive monies, including cheques payable "To The Bearer".

68. The foregoing example also makes crystal clear the risks any Bank who provides banking services to the Applicants assumes. It would be so easy for Scotiabank to become an unwitting accomplice to the Applicants who are willing to deliver cheques made payable "To The Bearer" at an address in a country which is notorious for money laundering.

What Obligations Will Be Placed on Scotiabank if They Were Required to Accept the Applicants as Customers

69. Scotiabank would be required to conduct appropriate due diligence inquiries in accordance with the know-your-customer provision of the *PCMLTF* and its Regulations.

70. If the Applicants were given bank accounts, both UseMyBank and the customers of UseMyBank using the service to transfer funds, would fall within the definition of third parties in the legislation. As a result, because the Applicants' accounts would be used by or on behalf of third parties, Scotiabank would be obliged to abide with sections 9 and 10 of the Regulations. The relevant portions of section 9 include:

> *9.(1) Subject to subsection (4) every person or entity that is required to keep a signature card or an account operating agreement in respect of an account under these Regulations, ...shall, at the time that the account is opened,* ***take reasonable measures to determine whether the account is to be used by or on behalf of a third party****.*
>
> *(2) ...where the person or entity determines that the account is to be used by or on behalf of a third party, the person or entity shall keep a record that sets out:*
>
> *(a) the third party's name and address and the nature of the principal business or occupation of the third party, if the third party is an individual;*
>
> *(b) if the third party is an entity, the third party's name and address and the nature of the principal business of the third party, and, if the entity is a corporation, the entity's incorporation number and its place of issue; and*
>
> *(c) the nature of the relationship between the third party and the account holder.*

71. Section 10 of the Regulations is very similar, but applies to every person or entity that is required to keep a client information record under these Regulations.

72. Scotiabank is bound to comply with both sections 9 and 10 of the *PCMLTF* Money Laundering Regulations. The Applicants' Scotiabank accounts were being used by or on behalf of third parties, namely, the banking customers whose accounts were being debited by the

Applicants. As a result, in order to comply with these Regulations, Scotiabank would be obliged to obtain information and keep records about all customers of the Applicants, including:

(a) the banking customer's name, address and nature of the principal business or occupation; and

(b) the nature of the relationship between the banking customer and the Applicants.

It goes without say that this would place an enormous administrative and due diligence burden on Scotiabank, in circumstances where the Applicants claim to have 20,000 Canadian customers. Moreover, as illustrated by my "Au Porteur" example, the information that is being gathered by the Applicants is unreliable and unverified by them. As a result, Scotiabank could not rely on information supplied by the Applicants to meet their obligations under the Money Laundering Regulations.

What Penalties Could Scotiabank be Exposed to if it was Required to Provide Bank Accounts and Other Services

73. The transactions involving money entering into Scotiabank's account in the Applicants' names could be classified as "suspicious" in that they are conducted with unknown persons, possibly in foreign jurisdictions (see for example, the ease with which I was able to register under the name "Au Porteur" with an address in a jurisdiction notorious for money laundering). Pursuant to section 7 of the PCMLTF, the Bank is required to report suspicious transactions to FINTRAC. If the Bank failed to report suspicious transactions, it would be subject to the following penalties, as described at section 75 of the PCMLTF, if convicted.

> *75.(1) Every person or entity that knowingly contravenes section 7 or 7.1 is guilty of an offence and liable:*

(a) on summary conviction,

(i) for a first offence, to a fine of not more than $500,000 or to imprisonment for a term of not more than 6 months, or to both, and

(ii) for a subsequent offence, to a fine of not more than $1,000,000 or to imprisonment for a term of not more than one year, or to both; or

(b) on conviction on indictment, to a fine of not more than $2,000,000 or to imprisonment for a term of not more than 5 years, or to both.

The Manner in Which the Applicants Transfer Money From Their Scotiabank Accounts

74. Mr. Grace has asserted that money is never transferred from a Scotiabank account in one of the Applicants' names to an off-shore Internet casino. The reasonable inference to be drawn is that money is bounced around from the Scotiabank accounts, to other bank accounts, and ultimately to an off-shore on-line casino.

75. I am not aware of any legitimate business purpose which would require the Applicants to transfer funds through multiple accounts and then finally to an off-shore location.

76. If the funds in question were, in fact, the proceeds of crime, the transfers could serve to make them difficult to trace by law enforcement.

77. Financial institutions within this "chain of transfers", once they became knowledgeable of the fact that a chain of transfers was occurring, would likely report these transactions as "suspicious" under the *PCMLTF* legislation.

Conclusion

78. The Applicants represent a very high risk banking client for any Canadian Schedule 1 Chartered Bank. As can be seen from the examples provided in this Affidavit including:

(a) the example with respect to the ease with which people can launder money using Sports Books;

(b) the real life scenario of the Ottawa Scotiabank customer who used GPay's services to transfer funds to an off-shore on-line casino and received monies payable by a Bank in Beirut, Lebanon; and

(c) the real life example of the ease with which I was able to register as a "Seller" with UseMyBank under an assumed name of Au Porteur (i.e. "To The Bearer") with an address in a country which is notorious for money laundering.

The following factors make the Applicants a high risk client for Scotiabank, including:

(a) the fact that the Applicant is a Money Services Business makes it a target for criminals wishing to launder proceeds of crime or terrorist financiers wishing to transfer money outside the jurisdiction;

(b) the Applicants appear to be transferring money to countries known to be "narcotic source countries" in that many of the offshore casinos serviced by UseMyBank are located in these countries, making the Applicants a likely target for criminals wishing to launder drug money;

(c) the Applicants appear to conduct business with countries with extremist/terrorist activity, making the Applicants a target for individuals wishing to transfer funds to those countries;

(d) the Applicants' client identification requirements as mandated by the *PCMLTF* and the Regulations thereunder are totally inadequate as evidenced by the "Au Porteur" example;

(e) the Applicants' business includes the remission of funds to off-shore Internet casinos which are themselves high-risk, due to the fact that they are usually located in jurisdictions with very lax money laundering controls;

(f) there is no evidence that the Applicants subscribe to the four accepted tenets of money laundering compliance, namely:

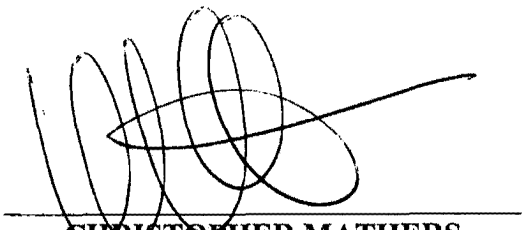
(i) the appointment of a compliance officer;

(ii) the development and application of compliant policies and procedures;

(iii) independent testing and review of compliance policies and procedures to test their effectiveness; and

(iv) an on-going compliance training program.

79. As a result of all of the foregoing, to require Scotiabank to offer banking services to the Applicants would place Scotiabank in an untenable position, both legally, under the PCMLTF, and with respect to the very real reputational risks associated with providing banking services to customers such as the Applicants.



CHRISTOPHER MATHERS

SWORN before me)
at the City of Toronto)
this 23rd day of November, 2005.)

A Commissioner for taking Affidavits

LISA M. CONSTANTINE

This is Exhibit "A" referred to in the affidavit of Christopher Mathers sworn before me, this 4th day of November, 2005

A COMMISSIONER FOR TAKING AFFIDAVITS

chrismathers inc.

crime and risk consulting

SUMMARY (RANGE OF EXPERIENCE)

In May 2004, Chris established chrismathers inc., a private crime and risk consulting firm in Toronto, Canada.

In 1995, following a twenty year career with the Royal Canadian Mounted Police, Chris joined the Forensic division of the international accounting firm, KPMG.

In 1999, he was appointed to the position of President of KPMG Corporate Intelligence Inc. where he was responsible for international due diligence and asset recovery operations.

Chris has provided advice and assistance to a variety of foreign corporations and governments on fraud and Anti-Money Laundering (AML) practices with specific attention to the corruption of employees in the financial sector.

He is regularly a guest instructor at several university MBA and Law programs where he addresses due diligence practices and the domestic and international implications of the *Corruption of Foreign Public Officials Act* (Canada) and the *PATRIOT* and *Foreign Corrupt Practices Act* (USA)

Chris is a popular media commentator and speaker on organized crime, terrorism and international business issues, appearing on major media outlets regularly in Canada and the US. He has served as a consultant on several feature films and documentaries relating to organized crime, espionage and money laundering. He is the author of the bestselling non-fiction book, CRIME SCHOOL: Money Laundering.

EDUCATION

Bachelor of Arts
University of Western Ontario
London, Ontario

Certificate in Advanced Police Studies
Canadian Police College
Ottawa, Ontario

Canadian Police College
Ottawa, Ontario
Certificate in Police Studies

AREAS OF SPECIALIZATION

Money Laundering
Fraud
Organized Crime
International Due Diligence
Public Corruption
Terrorism
Asset Recovery
Crisis Management

PROFESSIONAL AFFILIATIONS

Assoc. of Certified Anti-Money Laundering Specialists
Assoc. of Certified Fraud Examiners

PUBLICATIONS AND PRODUCTIONS

2004 *"Crime School: Money Laundering"*. Published in Canada by Key Porter Books and in the United States by Firefly Books Ltd.

2002 *"Physical Security and Biometrics"* – Canadian Broadcasting Corporation (CBC) business program "Venture". Wrote and hosted a segment describing the current advances in video and biometric technology as it relates to access/egress and computer systems.

2001 *"Don't Say A Word"* – Feature film. Provided consulting services and on-set consulting services to New Regency Productions on methods of bank robbery and safe attack

2001 *"Investment Frauds"* - CBC Venture. Wrote and hosted a television segment identifying the need for vigilance when accepting foreign investment.

1998 *"The Devil Inside"* - Canadian HR Reporter. Authored a feature article outlining the civil and criminal ramifications of insufficient reference checks of new employees.

1998 *"Bad Apples"* - Prevention of Corporate Liability. Authored an article describing the pitfalls associated to commonly accepted hiring practices in the North American private sector.

1998 *"Vehicle Theft an Epidemic in Canada"* - Canadian AutoWORLD - Authored a feature article describing techniques employed by organized automobile theft gangs.

1994 Authored research paper for RCMP, *"Disclosure in Criminal Cases: Contentious Issues and Potential Solutions."*

1994 Co-authored research paper, *"Systemic Solutions to Police Corruption and Organizational Deviance."*

EMPLOYMENT HISTORY AND RELEVANT PROJECT EXPERIENCE

KPMG LLP
1995 To May 2004 Toronto, Ontario
President, KPMG Corporate Intelligence Inc.
Vice-President KPMG Forensic Inc.

Reporting to the Chairman, Chris was responsible for the administration, sales, marketing and operations of the company, a wholly owned subsidiary of KPMG Forensic Inc.

He provided intelligence services and advice to corporations, governments and individuals in the areas of foreign due diligence and threat assessment, corruption, money laundering compliance, fraud prevention, foreign and domestic information gathering.

Selected assignments with KPMG included:

- Providing training and assistance to the Canadian Government's Office of the Superintendent of Financial Institutions (OSFI). OSFI is responsible for ensuring that all Canadian financial institutions are in compliance with Canadian money laundering legislation.

- Providing support and advice to the Canadian Department of Justice in their response to the constitutional challenge of the Proceeds of Crime (Money Laundering) Act by the Law Societies of British Columbia and Ontario.

Accomplishments:

- Designed and implemented training courses in money laundering investigation for government and corporate clients worldwide;

- Conducted international money laundering and terrorist financing investigations on behalf of foreign and domestic clients;

- Extensive international experience and foreign language skills with an emphasis on the Middle Eastern Gulf States, Latin America and South Asia;

- Conducted money laundering compliance reviews of financial institutions to determine their suitability as acquisition or merger targets;

- Provided advice and assistance on money laundering compliance and organized criminal activity to various foreign public sector organizations including:

Andorran Bankers Association (Andorra)
Bahrain Monetary Authority
British Chamber of Commerce (Hong Kong)
Canada / Europe Parliamentarians Association
Canadian Bar Association
Canadian Institute for International Affairs
Cayman Islands Bankers Association
Cayman Island Monetary Authority
Financial Stability Institute (Switzerland)
India Banking Association (Mumbai)
Investment Dealers Association (Canada)
Investment Funds Institute of Canada
Oman Monetary Authority
Ontario Securities Commission (Canada)
Public Policy Forum (Canada)
Qatar Bank Training Institute
Ryerson University (Canada)
Saudi Arabian Investment Authority
Saudi Arabian Monetary Authority
Singapore Institute of Banking & Finance
Society of Trust and Estate Practitioners (Cayman Islands)
South African Law Reform Society
Superbancaria (Colombia)
Superintendencia de Valores (Colombia)
Toronto Stock Exchange (Canada)
University of the British West Indies (Barbados)
University of Toronto (Canada)
University of Waterloo (Canada)
University of Western Ontario (Canada)
York University - Osgoode Hall Law School (Canada)

Royal Canadian Mounted Police, Toronto, Ontario
1975 – 1995

Conducting criminal investigations in Canada, the United States, Europe and the Caribbean, primarily in the areas of money laundering, drug trafficking and terrorism;

As the senior undercover investigator for the RCMP's Toronto Proceeds of Crime Section, Chris was responsible for all aspects of planning, development, administration and supervision of financial undercover operations; budgeting, training, establishment and maintenance of covert identities of undercover officers, establishment and maintenance of covert corporations and related bank accounts in Canada and abroad.

Accomplishments:

- Chris personally infiltrated numerous criminal organizations, both in Canada and internationally. He was the Canadian undercover operator in Operation "Green Ice," an international money laundering investigation conducted with the U.S. Drug Enforcement Administration and law enforcement from eight other countries. This investigation was directed at money brokers for the Colombian drug cartels;

- He was the lead Canadian investigator in Operation "OPBAT," a joint investigation with the U.S. Drug Enforcement Administration, that targeted money laundering activities of groups conducting cocaine offloading operations in the Bahamas and Turks and Caicos Islands;

- He initiated Project "OMNI," a joint investigation with Canada Customs. This investigation was the first "outbound" currency detecting program in Canada and was directed at the exportation of narcotics proceeds to South America and the Caribbean;

- Chris had responsibility for the design and implementation of specialized training for investigators of money laundering and proceeds of crime offences. He regularly lectured and conducted seminars for Canadian and foreign investigators on financial crimes, corruption and the establishment of storefront money laundering operations;

- He provided investigative and administrative assistance to foreign investigators in Canada pursuant to requests under Mutual Legal Assistance Treaties;

- He frequently provided expert (opinion) evidence to Canadian courts on matters relating to narcotics' offences and financial crimes.

chrismathers inc.
crime and risk consulting

Suite 2700, P.O. Box 136
The Exchange Tower
130 King St. West
Toronto, Ontario
M5X 1C7
Canada

(800) 693-8568

www.chrismathers.com

https://www.usemybank.com/SellerUpdate.asp?item=funds

Canada411

UseMyBank

auporteur@hotmail.com

Private Member Area - Saturday, November 19, 2005 - 10:25:23 AM

Overview | Tools | Profile | Reports | Contact Us | Log Out

Menu

- Overview
- Tools
  - Review Item
  - Add Item
  - Delete Item
  - Item Button
  - Seller Code
  - Affiliate Code
- Profile
  - Change Password
  - Payment Logo
  - Seller Profile
  - Buyer Profile
  - Affiliate Profile
- Reports
  - Seller Transactions
  - Buyer Transactions
  - Affiliate Listing
- Contact Us
- Member FAQ
- Logout

Note: all amounts are in local currency, unless otherwise specified.

Seller - Profile

Update Method of Disbursement

Please choose a method to receive funds, enter the information required, and select 'Update'.

( ) US Direct Deposit (ACH)/Canadian Direct Deposit (EFT) - Free + Bank Processing Fee ($2)

Bank Name:

Branch Location/Address:

Check/Cheque (ACH/MICR) Information:

Note: Enter ALL the numbers at the bottom of the check/cheque and include all spaces (eg. 095901 212010987 730029086 / 0959 01212010 7300290).

( ) Wire Transfer - $25 Handling Fee + Wire Bank Transfer fee (between $35-$70 depending on amount and location)

Wire Transfer Instructions/Account:

(•) Check/Cheque - $25 handling fee

Paid to the order of: Au Porteur

Update

What would you like to do?

- To change 'Password', click here.
- To Set/Update a Logo for the Payment page, click here.
- To view/update 'Seller Information', click here.

What's New

Apr 25, 2005
- Main Page Upgrade
- Enhanced tracking Upgrade
- General Fixes from last release

Coming Soon

- US/European Banks for all Sellers
- XML API for Approved Sellers

Suggestions?

Let us know what we can do to help!

Special Note

Thanks for all your suggestions. Please keep them coming we are trying to get to them as fast as we can!
- Joseph Iuso - CEO

Overview - Tools - Profile - Reports - Contact Us - Member FAQ - Log Out

This is Exhibit "C" referred to in the affidavit of Christopher Makeas sworn before me, this 1 day of November 2005

A COMMISSIONER FOR TAKING AFFIDAVITS

From : <support@usemybank.com>
Sent : Sunday, November 20, 2005 2:25 AM
To : <auporteur@hotmail.com>
Subject : UseMyBank - Disbursement Method Selected

Dear Au,

Your method of disbursement has been updated successfully!

For Sellers, you have now authorized UseMyBank to accept payments on your behalf.

Please read the instructions below carefully to ensure that the funds accepted on your behalf will be correctly sent to you.

You have selected the following Method of Disbursement:
Cheque - Free for 100 transactions or more per week, or $25 handling fee if less
- Free for Affiliates with $100 or more in disbursement
- Free for Sellers with 100 transactions or more a week, otherwise, a $25 handling fee will apply

In order for this method to be used, please verify the following information:

Cheque will be made payable to: Au Porteur

Mailing Address:
Au Porteur
24 Buada 6
Yaren, Yaren
66
Nauru

If this is not correct, please reply to this email indicating the appropriate information.

For Sellers, all disbursements are net of fees and will be disbursed every Thursday for payments received the previous week ending Friday. The minimum amount of the disbursement is $100.00. If this amount has not been reached by the end of the fiscal year ending December, any amount outstanding will be disbursed on first Thursday in January after the fiscal year end.

For Affiliates, all disburesments will be done on the first Thursday following the previous month end. The minimum amount of the disbursements is $100.00. If this amount has not been reached by the end of the fiscal year ending December, any amount outstanding will be disbursed on first

https://www.usemybank.com/SellerUpdate.asp?item=SAInfo

Canada411

UseMyBank - Private Member Area | (Untitled)

Menu

Overview
Tools
> Review Item
> Add Item
> Delete Item
> Item Button
> Seller Code
> Affiliate Code
Profile
> Change Password
> Payment Logo
> Seller Profile
> Buyer Profile
> Affiliate Profile
Reports
> Seller Transactions
> Buyer Transactions
> Affiliate Listing
Contact Us
Member FAQ
Logout

Seller - Profile

Seller Information View/Update

To change your information, change the appropriate field(s) below and press 'Update'.

Contact Information

First Name	Au
Last Name	Porteur
Contact Telephone	674 444 3181
Alternate Telephone	
Fax Telephone	

Contact Address

Address 1	24 Buada 6
Address 2	
City	Yaren
Province/State	Yaren
Postal Code/Zip	66
Country	Nauru

Other Information

Website URL	http://

Company Information

Company Name	
Company Type	Non-Incorporated - Other
Company Industry	Other

Company Address

Address 1	
Address 2	
City	
Province/State	
Postal Code/Zip	
Country	

Update

What's New

Apr 25, 2005
- Main Page Upgrade
- Enhanced tracking Upgrade
- General Fixes from last release

Coming Soon

- US/European Banks for all Sellers
- XML API for Approved Sellers

Suggestions?

Let us know what we can do to help!

Special Note

Thanks for all your suggestions. Please keep them coming we are trying to get to them as fast as we can!
- Joseph Iuso - CEO

Done

BETWEEN:

B-FILER INC.
Applicants

- and -

THE BANK OF NOVA SCOTIA
Respondent

Court File No. CT 2005-006

COMPETITION TRIBUNAL

AFFIDAVIT OF
CHRISTOPHER MATHERS
(Sworn November 23, 2005)

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

4049480