**Testimony of**

**Garry W.G. Clement**

**President & CEO**

**Clement Advisory Group**

**The House of Commons Standing Committee on Finance (Canada)**

**``Study on the cost, economic impact, frequency and best practices to address the issue of terrorist financing here in Canada and abroad``**

Good morning Chairman Rajotte and distinguished members of the Committee. Thank you for inviting me to testify at this hearing. Terrorist financing is a subject that is extremely important to me. I greatly appreciate the fact that you are taking the time to delve into this subject.

– *Prime Minister Stephen Harper* "Our Government is serious about taking action to keep Canadians safe. Recent attacks in Canada, which led to the deaths of Corporal Nathan Cirillo and Warrant Officer Patrice Vincent, as well as attacks in France and Australia, are reminders that the world is a dangerous place and that Canada is not immune to the threat of terrorism. Recent terrorist actions in Canada are not only an attack on our country, but also our values and our society as a whole."

There are few events in a lifetime that evoke deep seated emotion and vivid recollection. The terrorist attacks against the United States (U.S.) by al Qaeda on September 11, 2001 (9/11), and the recent events attacks in Ottawa are clearly some of those historic moments that remain frozen in our minds. At the time of the 9/11 attacks I was the Assistant Criminal Operations Officer in the National Capital Region and I witnessed first-hand how a major terrorist event can have a profound impact on our society and our lives. Canada's expanded military action in Syria will continue to keep us in the sights of extremists and therefore it is paramount we undertake a concerted effort to use all of our resources to choke off the funding of these terrorists groups.

I was very fortunate to have been involved in the RCMP`s proceeds of crime program in its embryonic stages starting in 1983. In addition I was one of only a handful of negotiators trained to be able to respond to a terrorist hostage situation. In total I have over 35 years of experience focusing on financial crime with a primary objective of thwarting money laundering and terrorist financing. Since retiring from the RCMP, I have provided consulting services regarding fraud, money laundering, cybercrime and terrorist financing. Many of my clients are in the financial services sector. Last week I was in Mumbai where I addressed the

International Council of Security Associations on the threat of cyber-crime, both from a criminal perspective and a terrorist financing risk.

My government investigative and private sector consulting experience has provided me a rare opportunity to understand two very distinct perspectives. For over 34 years, I had a law enforcement perspective. In that capacity, my perspective was government and investigative driven. For the last seven years, in my current position as a consultant, my perspective has shifted to one that is industry and compliance driven. This provides me with a unique understanding of the responsibilities, sensitivities, challenges and frustrations experienced by the government and financial sectors in dealing with anti-money laundering (AML) and terrorist financing considerations. There is a notable difference in perspectives. This is one of the many challenges we face in dealing with terrorist financing and other criminal problems.

Financial institutions spend millions of dollars each year erecting defences against money laundering and terrorist financing. Money laundering and terrorist financing are distinct areas of financial crime yet they share some common elements. Time and again, the financiers of terrorist acts have employed money laundering techniques to fund the young, the impressionable, and the desperate that pull a trigger or ignite a fuse. Erecting defences against terrorist financing, let alone detecting the transactions that finance acts of terror, can be extremely frustrating for a financial institution. Terrorists consider themselves at war, one with no rules or uniform. Terrorists camouflage themselves within a civilian population in order to unleash their fury upon unsuspecting targets or symbolic structures. If they can evade law enforcement and the intelligence community to fulfill their goals, they can also avoid recognition by a financial institution.

Identifying suspicious activity in financial institutions, especially involving terrorist financing, is extremely challenging. This is where understanding perspective is critically important. When it comes to identifying and reporting suspicious activity, you must consider the "who, what, where, when, why and how." Law enforcement typically focuses on the "why" as the most important element while financial institutions are most concerned about the "how." This is one of the areas where collaboration between law enforcement and financial institutions is paramount as thwarting a terrorist act requires real time information exchanges. We need to ensure a mechanism exists that would enable both CSIS and the RCMP to provide proactive sharing of potential alerts through confidential channels especially in regard to passport revocation and identified travel to high risk jurisdictions. Banks are in a position to provide meaningful information if their defined actions are approved and protected by public regulation. This I believe could be accomplished through the naming of a contact at each large institution following appropriate screening and designation. As we know individuals who have become radicalized react within short timeframes. In order to succeed,

individual terrorists, such as lone wolves, and terrorist groups must have access to money. They require funding in order to operate and succeed. Invariably, their funding sources will flow through financial institutions. To function, terrorists must have continuous access to money. Regardless of how nominal or extensive, the funding flow is operationally critical. Terrorists, like criminals, raise, move, store, and spend money in furtherance of their illicit activity. This is why PCMLTFA reporting requirements are essential to our National Security. This fact becomes more compelling in view of the actuality that finance is one of the two most significant vulnerabilities to terrorist and criminal organizations.

Terrorist financing is not fully understood and due to the amounts involved, it can be extremely difficult to identify. This is where government, through the interagency community engaged in terrorist financing, must interact more efficiently with the financial services sector to identify terrorist financing. It is possible for financial institutions to identify terrorist financing, but it is highly improbable in current circumstances. We must take continual actions that increase the probability factor, thereby increasing the possibility of identifying funding flows. The challenge confronting the government and banking community is to improve the effectiveness of the process. This is where the government needs to be more effective and efficient in the "how" of assisting financial institutions in identifying suspicious activity. I would argue that law enforcement and FINTRAC need to develop better real time feedback mechanisms to financial institutions about "how" terrorists use financial institutions and provide them with typologies that financial institutions could use for transactional monitoring.

We have all become far too aware of how terrorist groups, such as ISIL/ISIS are capitalizing on social media websites, not only to spread propaganda or recruit young persons but also as a means to raise funds. Globalization combined with the ability of terrorist organizations to use the internet and social media to attract, seduce and subsequently radicalize individuals to join "the cause" and wage jihad, or to support any other extremist action, exponentially increases the threat and effects of terrorism. Simply put, foreign fighters who are recruited to terrorist organizations expand the international reach of transnational insurgencies, as well as religious and ideological conflicts. This has allowed ISIL and others to generate and convert international support into funds. In February 2015, the Financial Action Task Force published a paper on funding methods by ISIL and one of the methods highlighted was international prepaid phone cards, where donors would buy prepaid cards and send the number of the card to the fundraiser via Skype. The fundraiser would then send the number to one of his followers in a country such as Syria and sell the number of the card with a lower price and the cash was later provide to ISIL. Prepaid cards may on the surface appear to be of little consequence but when it is realized they can be purchased by hundreds of individual sympathizers, combined they can lead to significant funding. In that regard, the new authorities proposed under c-51 with respect to a court approved take down order of terrorism promoting materials

off the internet and the new offence of knowingly promoting or advocating the commission of a terrorism offence, like funding a designated terrorist entity, may be quite useful.

Recently in a report from the McKenzie Institute (Hidden Within: Foreign fighters & the national threat *March 4, 2015 by* Colonel Bernd Horn) the authored stated *" For Western governments, foreign fighters also represent a hidden threat. Once they return home, or are ordered home by their respective organizations to carry on the fight, foreign fighters represent a cohort that is more experienced, more lethal and more dangerous and sophisticated than many of their domestic counterparts. They now represent a substantive menace, either as a group or as individuals acting in a "Lone Wolf " capacity. Canada is not immune. Government sources concede there are in excess of 130 known Canadian cases of individuals who have left the country to participate in training and / or actual operations with terrorist organizations. In addition, there are 80 known Canadian former foreign fighters who have returned home and are currently residing in Canada. The government's apprehension is that these foreign fighters exacerbate the potential for, and the effectiveness of, homegrown terrorism. The threat is even more ominous since identifying and tracking individuals leaving the country for nefarious purposes is not always easily accomplished as those radicalized and spurred to action do not fall under a single identifiable profile.*

*As they travel with Canadian, or other mainstream Western national passports, they can easily flow across international borders without being subject to the restrictions and visa requirements that are placed on many non-Western citizens. In the end, foreign fighters represent a growing threat that has implications for global stability as well as for domestic security. The solutions are far from simple and require a comprehensive global and domestic approach. As the barbarity and savageness of the Islamic State terrorist organization has shown, turning a blind eye to the cancer of foreign fighters and the organizations they support is an approach fraught with peril. Foreign fighters, although not all rallying to jihad or Islamic organizations, still represent a hidden peril that feeds transnational insurgencies, as well as a skulking national threat and, as such, they cannot be ignored."*

Terrorist financing is every bit as challenging today as it was in the immediate aftermath of 9/11. Law enforcement, regulators and intelligence agencies here, in Canada, and abroad, have achieved noteworthy and meaningful accomplishments. New proactive and progressive methodologies have been developed and implemented in furtherance of such efforts. When the government succeeds in implementing and executing proactive methodologies, the ability of terrorists to carry out operations is diminished. However, lingering concerns and the resiliency of terrorists to adapt to change, coupled with the ease of exploitation of systemic vulnerabilities in the financial sector, will perpetuate the challenge of addressing the issues presented by terrorist financing.

Today, we are faced with three significant challenges. The most significant crime problems we currently face in the financial services industry are fraud, money laundering and cybercrime. Fraud was magnified during the U.S. financial crisis and continues to represent a significant threat to our economy. The recent Charbonneau Commission underscored what happens when fraud is permitted unchecked. Money laundering encompasses all other criminal activity where the proceeds of crime are laundered through financial institutions. The key facilitation tools used in furtherance of fraud and money laundering are: wire transfers, correspondent banking, illegal money remitters, shell companies and electronic mechanisms. Cybercrime is what I consider the most serious threat and is a threat that is used by rogue governments, terrorists and organized crime and is the one crime that is 100% borderless.

Illegal money remitters represent a significant problem confronting Canada. When the sanctions were initiated against Iran, many Canadian banks closed any money service business that had dealings with Iran and they themselves closed many of the Canadian Iranian communities' accounts. What resulted was that the illegal money remitters capitalized and have successfully been moving money ever since. We must accept that as a country we allow many Iranian students each year to study in Canada and we have a very large Iranian community which needs to legitimately move money between Iran and Canada. Unfortunately this movement is now carried out in an underground economy which opens the door for both terrorist financing and criminal money laundering. Over the course of the last few years I have filed several intelligence reports relying on close Iranian contacts which have clearly established that illegal Iranian money remitters are operating freely in most large Canadian cities and I would suggest these same remitters pose a serious terrorist financing threat.

This has been an ongoing challenge. Many banks cannot identify customers who operate illegal money remittance operations and law enforcement at all levels do not have sufficient financial investigators to effectively investigate these illegal remitters. On the surface, they appear to be a legitimate business. However, like a jewelry store in Toronto, they actually functioned as illegal money remitters funneling money to high risk countries. Consequently, terrorist and criminal groups have used illegal money remitters in furtherance of their illicit activities.

Additionally sanctions against countries such as Iran caused entities to regularly use shell companies to hide beneficial ownership, as well as rely on correspondent banking and wire transfers to illegally move funds. The Lloyds Bank "stripping" case is a prime example of how correspondent banking was used by Iran as a facilitation tool. In this matter, Lloyds stripped SWIFT messaging information to hide Iranian bank identification in order to avoid U.S. banking monitoring detection. The Alavi Foundation case was an example of how Iran used shell companies to hide beneficial ownership in a New York City office building.

Both cases involved the use of wire transfers.

The use of electronic payment mechanisms is an area of growing concern regarding how terrorists move money due to the anonymity and instant settlement it affords. Electronic payment mechanisms are becoming more prolific and vulnerable to misuse by criminals and terrorists. Africa is a venue of concern for the growing use of electronic mechanisms.

Over several years I argued that the white-label ATM industry begs for regulation under the PCMLTFA. The industry argues that they provide appropriate oversight however my experience this is not the case. White label ATMS provide a laundering vehicle which can easily be controlled through a regulatory amendment mandating the reporting to FINTRAC of funds being placed in the private machines.

I would also urge the committee to look at regulatory amendments to enable the utilization of technology for the purposes of identifying clients in a non face-to-face on-boarding relationship. The current regulatory framework relies heavily on attestations which have proven to be fraught with some danger in light of the capability of the criminal element and the progress made by cyber criminals. With ongoing advancements in technology I would respectfully submit that identification can be effectively enhanced. The following passages that were in a report to the Canada Privacy Commissioner support this premise and I believe would better enable the effective identification of individuals:

*"Automated facial recognition involves the identification of an individual based on his or her facial geometry. For facial recognition to be successful, there needs to be a quality digital image of an individual's face, a database of digital images of identified individuals, and facial recognition software that will accurately find a match between the two. Of all biometric technologies, facial recognition most closely mimics how people identify others: by scrutinizing their face. What is an effortless skill in humans has proven immensely difficult and expensive to replicate in machines. But through a convergence of factors in the past few years, facial recognition has become a viable and increasingly accurate technology.*
*Digital images have become pervasive, through the proliferation of surveillance cameras, camera-equipped smart phones, and inexpensive high-quality digital cameras. Cheap data storage has led to massive online databases of images of identified individuals, such as licensed drivers, passport holders, employee IDs and convicted criminals. Individuals have embraced online photo sharing and photo tagging on platforms such as Facebook, Instagram, Picasa and Flickr. There have also been significant improvements in facial recognition technology, including advancements in analyzing images and extracting data.*

*Faces have been transformed into electronic information that can be aggregated, analyzed and categorized in unprecedented ways. What makes facial image data so valuable, and so sensitive, is that it is a uniquely measurable characteristic of our body and a key to our identity.*

By relying on technology an individual wishing to be on-boarded with a financial institution and/or MSB would be required to be interviewed over a medium which initially would enable the on-boarding company to in effect conduct a face-to-face interview and compare identification documents using the visual medium. Furthermore by utilizing a medium such as "Skype" the interviewer would be able to speak directly to the proposed client, visualize their identification documents, and take a photo of the proposed client, and where required, seek clarification on source of funds, background of individual and/or their business etc. I would suggest that this would eliminate some of the fraud/identity theft which our financial industry is exposed to, today.

Recently I have worked with both an MSB and one of our Big "5" banks wherein a substantial amount of money was defrauded due to a phishing program on a client of both institutions and the client's identify was hijacked. Had a process been available outside of the current requirements involving a use of technology to speak directly to the client, I would submit cases like this would not be as easily perpetrated.

I would further submit that we need this same software ability including face recognition biometrics at our border points which will assist authorities in capturing returning Canadians who saw fit to take up the terrorist cause and upon their return will likely be more radicalized.

The government has made consistent incremental progress in addressing terrorist financing. Individual agencies and entities responsible for terrorist financing have matured and are evolving. They have individually and collectively developed investigative methodologies to deal with the constant and emerging challenges. CSIS and the RCMP can point to enhanced capabilities however as Commissioner Paulson has stated the recent terrorist activities have resulted in the shift of resources to focus on these threats and as a result other organized crime activities have had to take a back seat. I would strongly urge this committee to recognize that the investigation of financial crime and in particular money laundering and terrorist financing demands a high level of expertise. I argued for several years that it took a highly skilled investigator a minimum of five years working in the money laundering arena to gain the necessary expertise and experience to competently carry out these complex investigations. During my tenure I can

state that the RCMP promotional system was a major stumbling block to ever achieving the goal of ensuring investigators remained in specialized areas. I am sure you will agree that if you need brain surgery you do not want a general practitioner to carry out the operation and therefore the same remains true for financial investigations. To fully understand the complexity of these cases the recent conviction of two money launderers in Quebec; Chun and Lech who provided money laundering for organized crime shows the dedication and perseverance required by both Crown and police investigators seeing this was a 10 year ordeal.

Notwithstanding the progress made I believe two reports clearly show that Canada has significant progress to make in the area of enforcement. First of all the "2010-2011 Evaluation of the Integrated Proceeds of Crime Initiative - Final Report" in which the following conclusions were tabled:

> *"While the Initiative is having an impact, the findings from the evaluation team suggest that it is not as efficient or effective as it could be. Through the course of this evaluation, the following challenges faced by the Initiative were identified: funding, turnover, training, governance, monitoring, communication, legal and relationships challenges.*
>
> *To meet its objectives in an efficient way, the Initiative requires close communications and collaboration among its partners. Indeed, the original concept of the Initiative focused on integration as a key feature of the Initiative. The evidence obtained through the course of the evaluation suggests that this core feature of the Initiative has faded somewhat over time to the detriment of its operation.*
>
> *The Initiative's operations have been adversely impacted by several human resource factors, including: some partners physically leaving the units (organizations are no longer co-located), staff turnover, vacant positions, recruitment difficulties, lack of seasoned personnel and insufficient training. These human resources factors need to be addressed so as to ensure that the Initiative is restored to a fully functional Initiative.*
>
> *Consistency and uniformity of performance data can be seen as a necessary hallmark of any integrated operation. However, an integrated monitoring system was not in place at the time of this evaluation. Furthermore, all of the Initiative's partners have their own reporting systems and tools, and no common standard exists among them. Steps need to be taken by the Initiative's partners to better monitor its performance using a consistent set of performance metrics.*
>
> *In summary, the lack of an overall strategy and business plan, communication and relationships among partners, human resources, integration, lack of performance indicators and a common monitoring system, etc. are factors contributing to less than optimal performance." (https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/vltn-ntgrtd-prcds-crm-2010-11/index-eng.aspx)*

The second report entitled " *FOLLOW THE MONEY: IS CANADA MAKING PROGRESS IN COMBATTING MONEY LAUNDERING AND TERRORIST FINANCING? NOT REALLY"* submitted in 2013 of the Standing Senate Committee on Banking, Trade and Commerce concluded in two of its recommendations:

1) The Committee's opinion is that changes are needed in response to global developments in money laundering and terrorist financing, advancements in technology and the need for public awareness about the Regime. From that perspective, the five recommendations made by the Committee focus on risk-based reporting and an adherence to global standards, and to create public awareness.

2) The federal government ensure that the Financial Transactions and Reports Analysis Centre of Canada and the Royal Canadian Mounted Police employ specialists in financial crimes, and provide them with ongoing training to ensure that their skills evolve as technological advancements occur.

The government must continuously identify and assess emerging trends and develop case typologies they can share with financial institutions. In so doing, the financial services sector can implement transaction monitoring strategies to identify patterns of activity consistent with the case typologies of criminals and terrorists. The government has not done this as consistently as they could have.

In general, law enforcement and the FINTRAC have not done as stellar a job of working in a public and private partnership as they think they have or they could. I do not make this comment lightly. When I was in the RCMP, I continuously fought to maximize liaison relationships. It was not until after my retirement from law enforcement and my consulting work with the financial services sector that I realized we could have done more and that more needs to be done. Law enforcement and FINTRAC should do a better job of listening and providing feedback to financial institutions in the form of "how" terrorists and criminal organizations use the financial system in furtherance of their illicit activities.

What is important, especially in dealing with more minimal dollar amounts, is identifying case typologies and using them to develop targeted transaction monitoring strategies. This leads to the need for more consistent collaboration between law enforcement and the financial services sector including through enhanced use of specialists. Organizations such as the Association of Certified Anti-Money Laundering Specialists, the Association of Certified Financial Crime Specialists and the Association of Certified Fraud Examiners provide ideal forums for regulators, compliance personnel and law enforcement to collaborate and network with colleagues from around the world. FINTRAC has recently had their personnel receive training preparing them for obtaining their certification from ACAMS however there is a void within

Canadian law enforcement who do not seem to place the same value on these networking and learning opportunities.

This type of initiative could be effectively used to identify terrorist financing. There are a number of scenarios that could be identified and targeted in a similar fashion. An example would be the case of a lone wolf terrorist who leaves Canada and travels to Syria to attend a terrorist training camp. During the time that this individual attends the training camp, it is unlikely he or she would incur any financial activity, virtually falling off the financial grid. The combination of travel to Syria, a high risk country for terrorism, and a gap in financial activity, could be identified by targeted financial monitoring in a financial institution.

A good friend of mine and the former head of the FBI Terrorist Funding program Mr. Dennis Lormel testified before Congress and outlined key points which he argued would increase the probability of identifying terrorist financing. I have reproduced these points putting them into a Canadian context, and added an additional point as follows:

1) The government and financial sector must recognize the importance of terrorist financing specific training. This is a dimension that is lacking on both sides, although more on the part of financial institutions. Without specific training, the ability to understand and disrupt terrorist financing is more difficult to achieve.

2) The government must develop a means to legally provide security clearances to select personnel in financial institutions in order to share limited intelligence information that could be scrubbed against bank monitoring systems to identify account or transactional information associated with terrorists.

3) A consistent and comprehensive feedback mechanism from law enforcement must be developed that demonstrates the importance of PCMLTFA reporting, especially the significance of Suspicious Transaction Reports (STRs). FINTRAC`s STR Review leading to highlighting findings is a good mechanism that provides insightful information. In addition, specific feedback from law enforcement to financial institutions concerning the value and benefit of PCMLTFA data, including STR filings, would have a dramatic impact on the morale of individuals responsible for STR reporting.

4) There must be an assessment by the government of all STRs related to or identifiable with

terrorism cases. Such a review would identify specific red flags that could be used as a training mechanism and more importantly, could be factored into identifying typologies that could be used for the monitoring/surveillance capabilities of financial institutions. In addition, a determination could be made as to why the financial institution filed a STR. In many instances, the STR was filed for violations other than terrorist financing. Understanding what triggered the STR filing; in tandem with how the STR ultimately was linked to terrorist interests would be insightful.

5) In addition to assessing STRs, the government and industry should collectively identify and assess as many case studies, of terrorist financing related investigations, as can be identified and legally publicly accessed. The case studies should be compared to determine what types of commonalities and patterns of activity exist. In addition, common red flags should be easily discernible. This type of case study assessment, coupled with the STR analysis, would provide more meaningful information to consider in identifying terrorist financing characteristics, especially in cases involving more nominal financial flows. This would enable financial institutions to more effectively use surveillance and monitor techniques to identify questionable transactional information.

6) A combination of PCMLTFA data, particularly STRs, combined with empirical and anecdotal information would enable the government and financial sector to collectively and unilaterally conduct trend analyses. This would be a significant factor in identifying emerging trends. On a government level, this would contribute to implementing investigative and enforcement strategies. On the institutional level, this would enable the financial sector to implement strategies to mitigate risk.

7) Law enforcement needs to have the necessary funding to carry out its full mandate so that terrorist financing does not diminish the need for organized crime financial investigations and recognition must be given to the need for specialization which should be subject of government mandated targeted goals.

Although the world landscape has changed, and methodologies have evolved in recent time, terrorist financing remains the same. In essence, terrorists must have access to funds when they need them in order to operate. It is incumbent that government agencies cooperate, coordinate and communicate on both an interagency level and with the private sector in order to deny terrorists from moving and accessing funds and thereby diminishing their ability to operate.

As President Obama explained, “Resolutions alone will not be enough. Promises on paper can’t keep us safe …Lofty rhetoric and good intentions will not stop a single terrorist attack. The words spoken here today must be matched and translated into action. Into deeds.”

I would again like to thank this distinguished Committee for affording me the opportunity to participate in this most important study. I would be happy to answer any questions or to elaborate on my statement.