

# **Terrorism Funding: Implications for the Legal and Financial Sectors**


Reid MORDEN\*

<b>I. MONEY LAUNDERING.....</b>	<b>370</b>
<b>II. SUSPICIOUS TRANSACTION DETECTION SOFTWARE .....</b>	<b>370</b>
<b>III. CYBER CRIME IS CURRENTLY THE FASTEST GROWING AREA OF CRIME .....</b>	<b>378</b>
<b>IV. LITTLE IF ANY APPLICABLE LEGISLATION .....</b>	<b>378</b>
<b>V. WHICH COURT HAS JURISDICTION?.....</b>	<b>378</b>

---

\* Chair, KPMG Corporate Intelligence Inc., Toronto, Ontario.



- 
- ◆ Recent Money-Laundering Legislation
  - ◆ Few Tools to Interdict Terrorist Funding
  - ◆ New Laws, New Muscle
  - ◆ Follow the Money Trail

Until recently, Canada had few tools to deal with terrorist funding, much of which is centred on:

- Money laundering
- Charitable donations, voluntary or otherwise

Within the past months, there has been significant catch-up in terms of legislation. Before September 11, Parliament had passed the *Proceeds of Crime (Money Laundering) Act* and had before it a pale equivalent of United Kingdom legislation to deal with charities acting as fronts for terrorist funding.

After September 11, things dramatically changed. Initially, the Government was clearly vulnerable with respect to its legislative base in providing powers for the freezing or seizure of terrorist related funds. In more or less analogous situations in the past, the Government had relied on a patchwork of legislated powers, scattered among the *Export/Import Control Act*, the *Emergency Economic Measures Act* and Canada's *United*

*Nations Act*. The trigger for activating the powers of this last piece of legislation was (and is) action by the UN Security Council. Fortunately for the Government, the Security Council had passed requisite resolutions. Otherwise, Canada would have been badly out of synch with its major allies.

After a review of its legislative and regulatory base, the Government responded with legislation, the most significant, to date, being Bill C-36 which covers both money laundering and charitable donations as sources of terrorist funding.

This legislation has implications for both the financial and legal sectors. With respect to the legal profession, two issues will touch both practicing lawyers and judges.

With respect to charities, there will be active participation by judges, perhaps using information which may—or may not—be made available to those affected. Lawyers will clearly be involved representing affected clients.

For their part, financial institutions which hold accounts of charities will be under a clear onus to ensure that those accounts are genuine and legitimate.

That said, given the stiff penalties and the unusual—at least in Canadian legislation—reverse onus in the money laundering legislation, this is the area where I believe the greatest challenges will be posed to both the legal and financial sectors.

### **The Impact of Canada's Money Laundering Statutes on the Legal And Financial Sectors**



In any event, THERE WILL BE IMPLICATIONS, especially for the legal sector.

The line between terrorism and organized crime is a fine one. Many of the criminal techniques that I will touch on today are being employed by terrorist groups in order to finance, as well as conceal, their illegal activities.

In following terrorists, like following criminals, looking at the money trail is not a bad rule of thumb and these are trails which will come into increasing scrutiny from law enforcement agencies and intelligence organizations. Illicit ways of making and manipulating money and flows of money are crucial to terrorists and the ways to do so are common to them as they are to criminals and organized crime.

## The Ethics Of It All

### ABA Proposed Changes - Model Rule of Professional Conduct 1.6(b)

- ♦ 1983 - "A lawyer may reveal [information relating to the representation of a client] to the extent the lawyer reasonably believes necessary...to prevent the client from committing a criminal act that the lawyer believes is likely to result in imminent death or substantial bodily harm."
- ♦ 1983 - rule allows an attorney to disclose confidential information in order to prevent a client from committing a crime that poses an "imminent" risk of seriously harming someone.
- ♦ 2002 - changes broaden an attorney's right to divulge the existence of circumstances that are likely to cause serious injury or death regardless of whether a crime has been committed.



### ABA's Ethics 2000 Commission

- ◆ "... recognizes the overriding importance of human life and the integrity of the lawyer's own role within the legal system.
- ◆ "...the current rule is "out of step with public policy and the values of the legal profession as reflected in the rules currently in force in most jurisdictions."

Others have spoken or will speak to the issue of the inroads which the legislation makes on the principle of solicitor/client privilege. I will only say that the reaction of the profession in Canada seems to be going in a different direction than that of the American Bar Association.

#### **I. MONEY LAUNDERING**

Until recently it was difficult to get anyone interested in the prevention of money laundering. The events of September 11 changed all of that. But money laundering is a difficult crime for financial institutions to detect.

#### **II. SUSPICIOUS TRANSACTION DETECTION SOFTWARE**

With the millions of transactions that take place each day, how is a financial institution supposed to detect suspicious, non-cash transactions from the thousands of different accounts it maintains? Without software, it cannot.

Money laundering is usually not a series of cash transactions. Since many banks may be dealing with the 3<sup>rd</sup>, 4<sup>th</sup> or 5<sup>th</sup> level of a money laundering transaction, the usual indications of criminality may not always be apparent. Software gives you the ability to create personalized client profiles based on transactions and input data.

It provides reports of suspicious account activity based on irregular transaction volume and amounts. It analyzes transactional activity to determine suspicious trends by account, branch, employee, date, type of transaction and country. It maintains a history of all account activity and reports for internal and external auditors.

But, it doesn't do everything. The following slides provide a whirlwind tour of vulnerabilities for both the legal and financial sectors. As the slides are presented, try to imagine that they represent the mindset of an auditor from FINTRAC, the Financial Tracking and Analysis Centre. FINTRAC is slowly becoming very active. Given its mandate, when it does reach cruising speed, it will be quite a powerhouse. It will have to determine how it uses its legislative levers but on paper, it has the almost untrammelled ability to walk into your offices and demand and receive things which you would normally consider to be private within the purview of your corporation or your practice. Think about it.


## Money Laundering Regs.

### Sec. 71. (2)

- ◆ Compliance Officer
- ◆ Compliance Rules
- ◆ Independent Testing
- ◆ Training

## What are "Reasonable Measures"?

- ◆ Verification of the identity of clients with foreign residency
- ◆ Client "Profiling"
- ◆ Common Sense
- ◆ "Healthy" Suspicion

- 
- ◆ To whom does the compliance officer report?
  - ◆ Are the compliance rules being regularly updated?
  - ◆ Are client identity verification procedures documented on each client file?
    - Domestic
    - Foreign

- ◆ Training
  - When was it provided?
  - Who provided it?
  - Were they qualified to give it?
  - Do you have records of who was trained?
  - Has the training been updated?

- ◆ Employee interviews
  - What is a suspicious transaction?
  - To whom do you report it?
  - Where are the forms?
  - When did you last receive training?



The new money laundering legislation will ultimately be reflected in company regulations. Perhaps mostly within the purview of financial institutions, there will have to be compliance officers, there will have to be written rules. There will have to be independent testing of those rules and there will have to be training. Somebody is going to ask, “So what reasonable measures did you take?” “What did you do about verifying the identity of your clients, particularly those with foreign residency?” “Have you done any client profiling?” “Have you actually used a bit of common sense, judgment?” (Moreover there is a debate in the wings over what really constitutes a “healthy” suspicion.)

Other questions FINTRAC investigators are going to ask is “Who does the compliance officer report to?” They are not going to be satisfied to hear that the compliance officer, who is probably a middle level official, reports to the chief administrative officer. They are going to want to see that he reports to somebody with the power to actually do something about his report and that means implicating the front office in a corporation or the managing directors in a practice.



## Areas of Risk

- ◆ Correspondent relationships
  - Foreign law firms
  - Foreign banks
  - Any changes in beneficial ownership
- ◆ Relying on the due diligence of another firm

Let me just touch on one particular area of risk. Correspondent relationships. Foreign law firms. Now many of you, I suppose, have been dealing with Buggins Buggins and Buggins from that lovely island from down south and that relationship may have developed over generations. This is a good time to take a look at Buggins Buggins and Buggins before you do any more business with them; particularly if they come from a jurisdiction which has a reputation for business practices or business ethics which differ substantially from those generally followed here. For example, do you know where the beneficial ownership of your

correspondent lies? To the extent that you believe you know it, are you relying on the due diligence of another firm? If so, don't continue this way. Do your own due diligence, either directly or through a professional third party.

*Financial Action Task Force - June 2001*

**Review to Identify Non-Cooperative Countries or Territories**

**“REINSTATED”**

- ◆ Bahamas
- ◆ Cayman Islands
- ◆ Panama
- ◆ Liechtenstein

kpmg

*Financial Action Task Force - June 2001*

**Review to Identify Non-Cooperative Countries or Territories**

**“FAIL”**

- ◆ Cook Islands
- ◆ Dominica
- ◆ Egypt
- ◆ Guatemala
- ◆ Hungary
- ◆ Indonesia
- ◆ Israel
- ◆ Lebanon
- ◆ Marshall Islands
- ◆ Myanmar
- ◆ Nauru
- ◆ Nigeria
- ◆ Niue
- ◆ Philippines
- ◆ Russia
- ◆ St. Kitts and Nevis
- ◆ St. Vincent and the Grenadines

kpmg

The OECD's Financial Action Task Force (FATF) keeps a close eye on countries which cooperate in being transparent about their financial dealings. There are four countries which have been reinstated on the cooperative countries list, but that is against seventeen which failed the exam for reinstatement.

## Do You Really Know...



- Your clients?
  - Line of business
  - Source of wealth
    - How much information do we really have?
  - History
    - Criminal record
    - Organized crime associates

## The Client Acceptance Process

- Does your organization have one?
- Is it effective?
- Databases
  - National
  - International

“As a matter of principle, we do not do business with politicians.”

Michael Thomalin -  
Barclays Private Banking, 1998

## Do You Really Know...

- Brokerages, banks and exchanges?
  - Ownership and control
- Organized crime control of banks
  - Russia
  - Caribbean
  - Mexico
  - Nauru
  - Cyprus



Do you really know with whom you are doing business? Do you know what their line of business is? Do you know what their source of wealth is? Do you know anything about them? My experience in dealing with the corporate community in Canada is that due diligence involves phoning somebody down in the accounting department to say, “Did they pay their bill last month?” And if the answer is yes, then we sign them on for another transaction. Does your organization have a client acceptance process? If you don’t, you should. And you ought to keep a database and have access to and use those available electronically and otherwise.

Let’s just touch on the various forms of financial institutions, especially brokerages, banks, and exchanges. In dealing with any of these kinds of institutions (and often you must), do you know who owns or controls them? We know various countries where organized crime actually controls banks. You don’t want to be involved in that and you should take serious measures to make sure that you, your practice, or your firm is indeed not implicated with them.

## Control of Financial Institutions by Organized Crime



Mexico

Amado CARILLO FUENTES  
@ "Senor de los cielos"  
Cocaine trafficker

died 97.07.05

photo date unknown

## Client "Profiling"



- Country of Origin
- Source of Referral
- Client Background
- Gaming/Lotteries
- Law Enforcement
- Military
- Government/Politics

How does it happen? For example, Amado Carillo Fuentes. A very nice man, unfortunately now deceased. He was a very successful cocaine trafficker with close links to various insurgent forces in Columbia. But he saw that he was going to have difficulty moving his profits so what did he do? He went out and he bought a bank. He bought a nice little Mexican bank. He worked the system extremely well. Beneficial ownership is something that people don't spend a lot of time checking and frankly, I think in a new, and much riskier, transparent world, it will be essential.

A related issue is client profiling. Take a look at where your clients are from. Gauge the reliability of your source of referral. Moreover, if your potential clients come from certain countries and have backgrounds in such areas as gaming or lotteries, law enforcement or the military, then *caveat emptor*.

A final digression.

### **III. CYBER CRIME IS CURRENTLY THE FASTEST GROWING AREA OF CRIME**

And it represents a series of techniques now being exploited by terrorists.

### **IV. LITTLE IF ANY APPLICABLE LEGISLATION**

Legislation has not kept up with the evolution of electronic crime. There is insufficient legislation or case law to provide guidance on what can be accepted as evidence or the manner in which it must be collected, preserved and presented to the court.

Laws, if they exist, are inconsistent from jurisdiction to jurisdiction.

Some countries simply can't keep up with the changes required.

How do we quantify the loss from an invasion of an individual's or a company's, privacy?

### **V. WHICH COURT HAS JURISDICTION?**

Even the most basic legal questions are still unanswered. In a recent case, a criminal in Canada used an Internet service provider in the Ukraine and then hacked into a server belonging to a Canadian company, but located in Antigua. He downloaded proprietary information and software, which he stored on a server located in Texas.

How do the courts decide where the crime took place?


Where is the bad guy?

Where is the victim?

Where are the computer servers?

Where is the evidence? Canada? Texas? Ukraine? Antigua?

Which law enforcement agency has jurisdiction?



## Conclusions

- New Laws Have Teeth
- Onus Is On The Legal And Financial Sectors
- Due Diligence, Due Diligence

To sum up, the new laws have teeth and the onus has in many respects shifted from the prosecutors to the professions and the sectors which we have been talking about to demonstrate that they have acted in compliance with the law. I think the prospect of several years in jail and several million dollars in fines should be enough for you all to take a moment to understand the legislation and what it may mean for you, your company or your practice.

A final word. Or words. Due diligence, due diligence, and when you've done that, do some more.