"Internationalization of Financial Systems and the Impact of Technology"

The Cambridge International Symposium on Economic Crime

September 8, 2004, Cambridge, England

John Sliter, Superintendent
Director, Integrated Market Enforcement Branch
Royal Canadian Mounted Police
1200 Vanier Parkway
Ottawa, Ontario
K0C 1M0

Technology and Globalization have been very good for many businesses, including our capital markets. Electronic funds are transferred instantly. In fact, our markets are a perfect example of technology and globalization working hand in hand. What happens in a Stock Exchange in Canada is instantly reflected in London or Japan. A lot of the international stock exchanges have virtually disappeared. Where there used to be an actual floor on the stock market, where people would talk and trade, over the past decade such facilities were, for the most part, replaced with cyber markets. In fact, those of us in law enforcement are often hard pressed to identify the jurisdictions where individual trade transactions actually take place.

Technology has given law enforcement new opportunities and new investigative tools, but, unfortunately, as we have heard by numerous speakers, it is also being used by criminals to set up quickly and commit serious crimes in relative obscurity.

Transnational crime is soaring to new heights like never before. In fact, when it comes to economic crime, almost all 'financial disasters', as I like to refer to them, have international implications. A criminal activity in one part of the world can have far-reaching effects in another.

The global interconnectedness of crime today is unlike anything we have ever seen before. And because of all of this, it became obvious that we need to start thinking in very different ways about the nature of crime. Some creativity is needed.

At a time when the pace of change is continually moving faster and faster, it's no longer good enough to react, to simply wait for threats to gather. We have to be much more pro-active and get out in front of these issues. We can't do that by building and maintaining our own little empires.

Quite simply, crime and criminals have transcended traditional barriers and today they see the whole world as their field of operations - and so must we.

What can we do? It is my personal opinion that we need to make use of technology to allow a greater focus on an integrated and intelligence-led approach**. This means, international coordination as we have never had before.**

We know that Big Business uses technology to think and act globally;
We know that Organized Crime uses technology to think and act globally; and
We also know that Terrorist Organizations use technology to think and act globally.

I would like to focus today on who is **not** using technology to think and act globally,

I will be commenting on how I am of the view that Law Enforcement could make better use of technology, but before I do, let's reflect for a moment on the victims of financial crime. There are many reasons why victims of financial crime, for the most part, are prevented from thinking and acting globally.

Imagine a victim of crime here in Cambridge, England trying to make a complaint of international crime to the local constabulary. I suspect that the exercise is similar to that in Canada or the United States, where it can be an exercise in frustration. First of all, they have to learn to whom they should report the crime and they are faced with a long list of law enforcement agencies, regulatory agencies and private sector financial institutions all having some form of shared responsibility and jurisdiction.

Should they be fortunate enough to correctly identify the law enforcement agency of primary jurisdiction, they often find that they are asked to produce a completed court brief and perhaps a full forensic accounting analysis before the agency wants to hear about it.

Victims of crime have a strong motive for reporting and therefore a good deal of the time they will go to the time and trouble to ensure that their incident gets reported. But let us move on and consider concerned citizens who simply are observers of financial crime who would like to see some accountants and lawyers go to jail.

I would suggest that our current reporting systems allow for neither of these key stakeholders to international financial crime to make use of technology to think and act globally.

So what can we do…?

For one, we require a culture in which 'whistle blowing' is strongly encouraged. Next, we need to couple that with a crime reporting system that is able to get over the high hurdles caused by numerous regulatory borders and concern for sovereignty.

Please allow me to share what might be considered as a couple of examples of best practices from Canada.

Firstly, I am proud to say that the Government of Canada has recently enacted some new 'whistle blowing' legislation that dictates employers, who intimidate employees coming forward with information, could face prosecution and up to five years in prison. ***Whistle Blowers should be encouraged, and they are in Canada.*** Our new Canadian law, in addition to creating criminal penalties for insider trading and threats against whistle blowers, also increases maximum sentences for existing fraud offences and makes it easier for the police to obtain information from people not directly under investigation.

Secondly, we recently created a web-based reporting system in Canada entitled RECOL (an acronym for ("Reporting Economic Crime On-Line") that is linked to various levels of law enforcement and regulators at the provincial, federal and international levels. After 7 months of operation in April of this year, RECOL reported that we had received over 1,700 complaints from around the globe and from Canadians reporting suspects around the world. Over 400 of these complaints (valued in the hundreds of millions of dollars) were automatically and electronically sent to the Internet Fraud Complaint Centre in the United States. Furthermore, through the use of some sophisticated prioritization software, almost 20% of these complaints were unread by human beings

and simply deposited into various Provincial, National and International Intelligence databases. **This is an excellent example of using technology to create a model of integrated policing on an international basis.** From the perspective of capital markets in particular, I am pleased to say that we now have links to RECOL from several of our Canadian Securities Commissions and are receiving a significant number of complaints pertaining to "investment fraud". Further information can be found by visiting www.recol.ca.

All of this technology has also presented law enforcement with serious human **resource** challenges.

"High end" criminal activity like we see in these sophisticated financial crimes, means we need to produce more police officers with highly specialized technical skills. It can be very difficult to attract and retain such expertise.

Over the past couple of years, I have been involved in the implementation of a new initiative entitled "Integrated Market Enforcement Teams" or "IMETs."

The IMETS represent a different way of doing business.

Our IMET teams are made up of highly skilled RCMP investigators, accountants, lawyers and other investigative experts working together to detect, investigate and deter serious capital markets fraud. Approximately 50% of the personnel are civilian as opposed to law enforcement. They work very closely with securities regulators, federal and

provincial authorities and local police. We also encourage secondments from other law enforcement and from all levels of regulation. This is the crux of our new IMET Teams— integrated teams designed to respond swiftly to sophisticated financial crimes.

When breaking the mold on traditional approaches to complex investigations, we experienced many challenges, a prime one I mentioned being the 'attraction and retention' of expertise. We have some successes to share - particularly in the area of using competency profiles to staff key positions. This relates to the requirement to produce more police officers with the highly specialized technical skills I spoke of earlier. Some of these challenges, and our response to same, are whole other topics amongst themselves that I will save for future discussions. Let's just say that we knew we had to get the best and brightest white-collar crime investigators on the teams. Investigators that are very adept at using the latest technology. In one sentence I can tell you that the process of competency based selection ensures that only the most qualified candidates are able to apply for a given position and this is followed by an interview process that allows us to "pick the best of the best" so to speak. I will tell you that we are very impressed with our current level of expertise and I anticipate reporting significant investigational and prosecutorial success at future symposiums.

International Requirement **for Global Cooperation**

In Canada, we are generally optimistic that we have come a long way in the past few years in strengthening enforcement and reassuring jittery investors, but we know that there is still much more to do.

Our Canadian RECOL system of complaint distribution is being used as a pilot for the G8 Law Enforcement Projects Sub-Group ('LEPSG') to encourage more and more countries to join us in an international intelligence sharing project. We are using the Internet to ensure that all types of complaints of economic crime such as Insider Trading, Telemarketing and even Corruption are shared with all of law enforcement, regulatory and private sector agencies of legitimate interest. Just as we have new legislation to encourage 'whistle blowing' in Canada, we view our RECOL system as a model capable of distributing that information internationally in the form of real time 'hot' tactical intelligence.

Just as nothing is stopping victims of financial crime from creating packages of information in their possession, and mailing them to law enforcement agencies around the world in order to 'blow the whistle' on crime, there is nothing stopping us from using the Internet to build a sophisticated electronic mail distribution system to ensure that the information is shared quickly and widely by all.

An intelligence-led approach is not simply about monitoring situations and sharing information with other law enforcement agencies, it is about involving the people who know their community and understand it. People like those having a legitimate interest from the private sector and most importantly, the actual victims of the crimes, be they corporations or individuals. Really good international intelligence requires total integration and crossing all borders.

So, I believe there is still much work to be done on the subject of global cooperation. More than ever, intelligence should flow across borders and date lines. We must use our imaginations to anticipate the crimes of tomorrow. The unprecedented pace of change means that we cannot simply ask, "What worked in the past and how do we improve it?" We need to think about "what is required today, and, what will be required tomorrow?", to protect our corporations, financial institutions and capital markets.

Relying on 'current practices' will not prepare us for the future. We have to be ready to welcome technological change and respond to it. There is no doubt that these challenges are complex, yet I am confident that if we use technology wisely, and to our advantage, we can triumph.

Particularly, if we work together.

Thank you.