The Internet and Criminal Law—The Detection and Investigation of Stock Fraud

John SLITER*

* Inspector; officer in Charge of Policy & Program Management, Economic Crime Branch Federal Services Directorate, Royal Canadian Mounted Police.

Please allow me to begin with a short and somewhat amusing story that I believe encompasses some of the spirit of the topic of this conference, "Science, Truth and Justice." It also provides a good example of a genuine on-line solicitation that is on the Internet today.

> "The Second Coming Project is a not-for-profit organization devoted to bringing about the Second Coming of Our Lord, Jesus Christ, as prophesied in the Bible, in time for the 2,000th anniversary of his birth. Our intention is to clone Jesus, utilizing techniques pioneered at the Roslin Institute in Scotland, by taking an incorrupt cell from one of the many Holy Relics of Jesus' blood and body that are preserved in churches throughout the world, extracting its DNA, and inserting into an unfertilized human egg, through the now-proven biological process called nuclear transfer. The fertilized egg, now the zygote of Jesus Christ, will be implanted into the womb of a young virginal woman (who has volunteered of her own accord), who will then bring the baby Jesus to term in a second Virgin Birth.
>
> If all goes according to plan, the birth will take place on December 25, 2001, and all calendrical calculations will begin anew. How can this be possible? 1. Modern cloning technology enables us to clone any large mammal—including humans—using just a single cell from an adult specimen. 2. Throughout the Christian world are churches that contain Holy Relics of Jesus' body: his blood, his hair. Unless every single one of these relics is a fake, this means that cells from Jesus' body still survive to this day. 3. We are already making preparations to obtain a portion of one of these relics, extract the DNA from one of its cells, and use it to clone Jesus. No longer can we rely on hope and prayer, waiting around futilely for Jesus to return. We have the technology to bring him back right now: there is no reason, moral, legal or Biblical, not to take advantage of it. IN ORDER TO SAVE THE WORLD FROM SIN, WE MUST CLONE JESUS TO INITIATE THE SECOND COMING OF THE CHRIST. The Second Coming Project is soliciting contributions and donations

> to help us in our quest. Time is short! We must have a fertilized Jesus zygote no later than April of 2001 if Baby Jesus is to come to term on the predicted date. Please send all contributions to: The Second Coming Project, P.O. Box 295, Berkeley, CA 94701.

While this may sound amusing, we have observed chat room conversations in which people express outrage that attempts are being made to clone Christ. There are believers and therefore, we also expect some people may be contributing funds to the scheme.

Yes, the Internet is a wonderful medium for such schemes and now I will focus my comments on how it affects the detection and investigation of stock fraud. First let me say that technology, and in particular the Internet, has had a profound effect on the process of traditional stock trading. In recent years we have seen the investor obtain the ability to purchase and sell their securities on-line. Trading accounts in the United States are expected to surpass 20 million and the value of assets to reach $1.5 trillion by the year 2005 (Forester Group Consulting). Furthermore, in 1998, approximately 22 % of all US securities transactions were conducted over the Internet compared with virtually no such transactions in 1995.[1]

The Internet has become very popular among investors because it allows them to buy and sell securities from their personal computers, enjoy lower trading commissions, and gain ready access to market research. Information (both bad and good) travels literally at the speed of light and allows for consumers to make better informed investment decisions. In fact, it is the optimistic opinion of some that we may be approaching that euphoric state of economic "perfect information." However, it would be remiss not to acknowledge opposing views that prefer to think of the market research available on the Internet as "perfect disinformation."[2] Another highly respected criminologist recently noted that perhaps some Internet Websites should be suffixed with the annotation of "dot.con" instead of "dot.com."[3]

---

1 R.J. Hillman, "Testimony Before the Permanent Subcommittee on Investigatios Committee on Governmental Affaires" *U.S. Senate,* Washington D.C., March 22, 1999 at 1.

2 T. Naylor, Personal Meeting Statements made at RCMP Headquarters, Ottawa, September 28, 2000.

3 M. Levi, "Eighteenth Symposium on Economic Crime" Cambridge (U.K.), September 13, 2000.

Yes, every rose has its thorn, and unfortunately, the Internet also provides fraudulent operators with a new and efficient medium to defraud investors of billions of dollars. Securities fraud perpetrators find the Internet particularly attractive because they can instantly communicate with millions of potential victims via professional looking Websites that appear to offer legitimate investment information, on-line newsletters, or e-mail—at far lower costs than traditional means of communication, such as the telephone. On-line discussion groups and chat rooms further allow anonymous promoters to post false news and buy/sell into the interest they have created whilst operating from nearly any undisclosed location in the world; thereby evading regulatory and law enforcement authorities. In past eras, this form of market manipulation would have taken months, even years. It can now be done in mere minutes.

Simply put, the Internet is a very efficient medium to perpetrate traditional securities frauds. On-line stock manipulation of international proportions has been a significant problem as long as people have been using the Internet to get financial information.

Consider the following examples:

In April of this year, a tree-trimmer from Los Angeles masqueraded as a financial analyst and made $1.4 million through a "pump and dump" scheme involving eConnect shares.[4] For those not familiar with this term, he simply posted false news through on-line reports that were purportedly "objective analyst reports" ("pumped") and then sold heavily into the interest he created ("dumped").

Similarly, a few months later, an individual in California used a technique referred to as "cybersmear" and issued a press release warning that the CEO of Emulex Inc. had resigned and that the corporate earnings had been significantly overstated.[5] When the market opened the following morning, the instigator sold heavy into the ensuing melee. Shareholders lost $1 billion (U.S.) dollars in the first hour of trading!

---

[4] M. Martin-Higaldo, "Organized Crime Targets Small Company Stocks" *Reuters,* Washington D.C., September 18, 2000.

[5] A. Berenson, "On Hair-Trigger Wall Street: A Stock Plunges on Faxe News" *The New York Times*, New York, August 26, 2000 at A1.

It is important to stress that these offences are not being committed by persons who might be thought of as traditional market players. For example, there is another recent story of a 15-year-old, 10th grader from New Jersey, who would send misleading notes about stocks he owned to various "Yahoo!" bulletin boards, hoping his words would cause share prices to soar. Then, in the morning before he left for school, he would place sell-order limits, ensuring that while he was in class he could profit from the previous evening's mischief. Profit he did—he earned approximately $270,000 (U.S.) for his efforts.[6]

We have also seen cases where organized groups of individuals have made significant profit based on false news.

A few years ago, thousands of Bre-X shares traded hands based on on-line rumour focused on whether a proposed deal with Barrick Gold Corp. had fallen through or not. Prior to those specific rumours we witnessed many Canadians become millionaires and many Canadians lose millions on the on-line Bre-X speculation as to whether there was actually any gold in the Busang jungle.

In June 2000, we also saw RT Capital, a branch of the Royal Bank of Canada, admit to manipulating the price of 26 stocks through the practice known as "high-closing."[7] RT Capital manages pension funds for dozens of Canadian corporations, including Air Canada, Alcan Aluminium, Noranda Inc. and Sears Canada Inc. In spite of market manipulation being a Criminal Code offence, no individuals were charged and the matter was treated as a regulatory issue and handled by the Ontario Securities Commission.

As if the economic threat from these groups was not enough, we are now hearing of cases where organized crime is also getting involved in on-line market manipulations. There are allegations that Russian organized crime was laundering funds through the TSE listed company YBM Magnex International Inc.[8]

Last month, a U.S. congressional hearing was told that Eurasian and Eastern European crime gangs are infiltrating the small-cap stock market using the Internet to sell investors bogus shares of stock at inflated prices.

---

6 S. Craig, "15-Year-Old Scams $272,826 by Rigging Stocks on Internet" *The Globe and Mail*, Toronto, September 21, 2000 at A1.

7 K. McArthur, "The Regulators Strike Back" *The Globe and Mail*, Toronto, June 30, 2000 at B1.

8 D. Crane, "Our Second-rate Financial Image is Showing" *The Toronto Star*, Toronto, July 6, 2000.

Just a few weeks ago, CNN ran a report that organized crime was moving beyond its traditional strongholds in New York, namely garbage hauling, construction and the Fulton fish market. It was suggested that repeated government crackdowns on organized crime in those industries prompted the Mob to look elsewhere: Wall Street. It was also noted that while no industry group nor any government agency had ever totalled the damage done by dozens of Mob-influenced brokerages, it has been estimated that during the last decade investors have lost close to a billion dollars in stock market scams run by Mob-directed brokers. In June, federal prosecutors in New York announced the single biggest round-up of alleged Mobsters and corrupt brokers ever; 120 people, including a dozen organized crime figures were arrested in Operation Uptick.[9] For those that might think this is strictly an american problem, it should be noted that two stock brokers arrested for participation in this securities fraud were operating from Vancouver, British Columbia.[10]

The Internet has also provided an opportunity for a new type of securities fraud—Website identity theft and fraudulent solicitation. This scheme involves a person hacking into a legitimate company Website and slightly altering their information in order that victims are now encouraged to send funds to a new address—a mail drop. In 1998, a company called "Turner Phillips" was able to make it appear that they were a member of the Investment Dealers Association, three Canadian Stock Exchanges and Nasdaq in the United States. Suspects hacked into the Website of a legitimate Canadian investment dealer that is a member of these self-regulatory agencies, copied all of the information, superimposed the name Turner Phillips onto that firm's data, and then posted the material to its own site. The suspects then contacted prospective victims in Sweden over the telephone and referred them to the doctored Website for more information on their firm. Investigators were unable to identify where the telephone calls originated from. Although Turner Phillips said its head office was in Vancouver, British Columbia, all it had in that city was a mail drop and a telephone answering service. Calls placed to the Vancouver number were forwarded to a location in Washington State and then from there to another location. Incoming mail was forwarded to an address in Ontario. The RCMP was able to identify three registered companies entitled "Turner Phillips" in

---

9 F. Guida, T. Guida & A. Dodds, "Organized Crime on Wall Street" *CNNFN*, New York, September 20, 2000.

10 D. Hasselback, "Brokers to Plead Guilty in U.S. Scam" *National Post*, Toronto, June 30, 2000 at C8.

all of North America but they appeared to be legitimate firms in Alabama, Texas and Virginia.

Once this scheme was identified, the legitimate firm was forced to remove its Website from the Internet. This particular fraud resulted in the loss of millions of dollars worldwide and it is important to note that it is not the first time that it has been used. Canadian securities regulators identified an almost identical scheme a year earlier originating from a firm registered in Ireland.

The above scenarios demonstrate the potential for these very lucrative and international schemes, a potential that is further amplified by the ability to solicit interest or even "telemarket" through the Internet via the technique of "spamming." In the current on-line world, a securities salesman is able to reach hundreds of thousands of people with a single message. In fact, with a couple of keystrokes, a couple of accounts, and a macro or two, they can make it appear that many people are posting on many different systems, all talking up a stock. An individual has never been able to reach so many people, so easily, quickly, or inexpensively.

I. INVESTIGATIVE CHALLENGES

The following comment by U.S. Attorney General Janet Reno describes the current state of affairs with respect to the Internet and Law Enforcement very well:

> "We are in the midst of a technological revolution that is changing the world right before our eyes. The Internet is changing everything. Today, we can communicate, share information and transact business with others around the world almost instantaneously. Undoubtedly, these new technologies will continue to enhance our lives in ways that we cannot fully imagine. However, these same technologies are already posing an unprecedented challenge to law enforcement, both domestically and abroad."[11]

Perhaps the greatest challenge to law enforcement when dealing with the Internet is that of jurisdiction. Consider the story of the World Stock Exchange. Two men from Edmonton, Alberta, were charged in October 1998 with breaches of the *Alberta Securities Act* that relate to a scheme whereby they created a world stock exchange in cyberspace. They set up a Website called the "World Stock Exchange" in which they solicited companies to

---

[11] J. Reno, "Attorney General's Cyber Crime Plan" *The Prosecutor,* Oxford, at 21.

publicly list and trade securities around the world. Companies could list on the World Stock Exchange for fees ranging from $5,000 to $20,000 U.S. The two persons ignored repeated requests to take down the Website, and changed Internet service provider from an Edmonton company to one in the Cayman Islands and later to one in Antigua and Barbuda. None of the listed companies filed prospectuses in Canada. The Website described the exchange as follows: "The World Stock Exchange was incorporated and established in a manner that ensures that it does not fall under the securities regulation of any country."

In June of this year, the Toronto Stock Exchange announced that they were involved in global talks that involved ten stock exchanges proposing a round-the-clock stock exchange to operate worldwide.[12] The idea is to create a pool of large global stocks that can be traded on any one of the 10 exchanges in the alliance during local business hours, making it easier and perhaps cheaper for investors to trade. Should this global stock exchange go on to become reality, it will undoubtedly provide an interesting jurisdiction challenge to both regulators and law enforcement.

It has been two years since the debut of the "World Stock Exchange" in 1998 and things have become much more complicated since then. In the investigation of complex networks we have observed access to be both wireless and remote. As the cost of data storage became more and more economical we have seen numerous on-line entities offer remote Websites with free data storage. This allows persons involved in illegal activity to log on to any computer in the world and store and retrieve their day to day business records from secret off-shore locations—locations that are sometimes unknown even to the user. This free off-site storage capability is something that is readily available today on the Internet. One example entitled "WS-FTP" is a file transfer protocol that is very easy and convenient to use.

---

[12] R. Ferguson, "TSE in Global Market Talks" *The Toronto Star*, Toronto, June 8, 2000.

There are also several issues related to electronic evidence that I could spend several hours discussing. I will take a moment to refer to one particular challenge that pertains to evidence—sometimes we encounter too much. Consider the latest DVD technology that accommodates 17 gigabytes of data on a single disk. Compare that disk to a paperback novel of 300 pages. At 36 lines per page and 60 characters per line that would approximate 650,000 characters per book. This would suggest that our 17 gigabyte disk is the equivalent of approximately 80,000 books. This dictates that the police use computers to search computers. How our courts respond to this use of "virtual" police officers remains to be seen—we are evolving toward the use of search programs encoded with artificial techniques and it is these programs that will be asked to determine what information is relevant and what is not.

All of this translates into the fact that the laws of the Internet are still evolving around the world. In the meantime, law enforcement is left without direction from the courts and hence has not developed strong guidelines and policy that are customarily derived from such law. Everything is moving so quickly that we are forced to adopt a "que sera sera" attitude and a "learn as we go" approach.

II. THE POLICE RESPONSE

Some might think that the problems associated with international securities fraud on the Internet are overwhelming. I would say that, in spite of all the challenges I have referred to, I believe that the RCMP is up to the challenge and that we are ready to make our move.

Firstly, I would like to make two points. One, our RCMP Economic Crime Program is much in favour of e-commerce and we are continually searching for ways to help prevent e-fraud. We believe that the strength of the Canadian economy will depend on our ability as a country to adapt to e-commerce. We see our role as one of a guardian—who will seek to protect and enhance the image of e-commerce as a safe method of doing business and not one to stifle nor discourage further development through fear-mongering.

Secondly, while the criminal element may have benefited from advances in technology, so have the police. We could provide a vast number of examples of how police work has been made easier through advances in technology. Let me give you a few specific examples of what the RCMP has done to deal with Internet securities fraud.

III. EDUCATION AND PREVENTION

We regularly post examples of typical Internet schemes onto the RCMP Website and we follow these with "Alerts" on those schemes that we have become aware of, reviewed, and are of the opinion may constitute criminal behaviour. Occasionally, we have also monitored postings in chat rooms and found ourselves in the fortunate position where we could alert prospective victims before they fell victim to fraud. In fear of making this sound too good, I must also say that we have suffered from a decade of severe economic restraint and have not had the luxury of monitoring chat rooms with any regularity.

IV. ENHANCED USE OF TECHNOLOGY

Apart from the normal police use of document scanning and electronic search and seizure techniques, the RCMP has also taken a leading role in the development of the Market Integrity Computer Analysis system ("MICA"). MICA was developed by a consortium of partners from the provincial securities commissions, stock exchanges, the Investment Dealers Association and the RCMP. The system is now fully operational and allows administrators and investigators to review and analyze trading activity pertaining to specific securities and produce subsequent evidentiary summary reports for use in both administrative proceedings and criminal prosecutions. MICA is a good example of complex investigator techniques being encoded into an expert computer system.

V. NATIONAL ECONOMIC PROFILING SERVICE ("NEPS")

Economic Crime Branch has also developed a National Economic Profiling Service that involves the preparation of economic profiles on individuals and public and private companies. The information in each profile is derived from publicly available information such as Lexis Nexis, Canada Stockwatch, the Office of the Superintendent of Bankruptcy database, and the Internet. Profiles may include the names of companies an individual has been involved with and their role within each company, biographical information (names of spouse and children, education, interests, past and present employment, date of birth, etc.) and news articles. There are

a great many professionals, some of whom are involved in criminal behaviour, who have created personal Websites, and who take the time to post their résumés on the Internet.

VI. RCMP "VIRTUAL" DETACHMENT: INTERNET FRAUD REPORTING CENTER

The RCMP Economic Crime Branch is currently poised to commence building a new Internet Fraud Reporting Centre that will accommodate the complete electronic reporting of crime to a central and national location. This centre will be very similar to the U.S. Internet Fraud Reporting Centre; however, we hope to expand the reporting to include all types of crime, as opposed to just fraud. Our vision is to build a genuine "virtual" detachment that will be responsive to the needs of all law enforcement in Canada by receiving detailed complaints and, by using artificial intelligence techniques, forward such to the appropriate jurisdiction via the most advanced electronic means available to the receiving police jurisdiction.

While on the subject of technology, I would like to make a plea for all those associated with the Canadian Justice system, who have not already done so, to open their minds and enhance their own use of technology. Think of a decade down the road, which incidently is 40 Internet years. How will our whole end-to-end justice system evolve? We are now generally accepting of the concepts of electronic disclosure, video testimony and, at least in some courts, the use of artificial intelligence in police computer systems. Think in the future what a fully electronic e-court might look like! I have described a move toward virtual detachments and virtual police officers. The most valuable police officers will no longer be those that are the most accurate shooters nor the strongest in self-defence. The ideal police officers of the future will be those that are the fastest on the mouse. I wonder what we might expect in relation to virtual lawyers and virtual judges.[13]

---

[13] For further discussion on the subject of electronic courtrooms see report entitled *Design of court systems and legal information systems—Proceedings*, Vienna, April 1999 Internet site: http://book.coe.fr/GB/CAT /LIV/HTM/l1628.htm.

VII. ENHANCED ENFORCEMENT

Finally, I would like to make a plea for general support of our plea for enhanced enforcement. The RCMP has been criticised by the media in recent years for not actively pursuing criminal code investigations of market frauds in Canada.[14] We openly admit that we are not in a good position to combat complex securities frauds. In fact, it has been reported that Canada is developing a bit of a reputation as a safe haven for securities fraudsters.[15] The RCMP has slowly divested itself of securities fraud enforcement and lost the much required expertise over the past decade to the point where we have almost no one left capable of operating the MICA software. We are now reduced to somewhere between ten and fifteen securities fraud investigators across the country.

However, this past year the RCMP has circulated a proposal entitled "A Proposal for a New Enhanced Role for the Royal Canadian Mounted Police in the Canadian 'Virtual' National Securities Commission." In recognition of the importance the integrity of the Canadian Securities Industry has on the overall Canadian economy, we are most anxious to rebuild a strong and effective police presence in the role of criminal enforcement for the securities industry. **We must bring back a genuine threat of investigation, prosecution and potential incarceration.** To that end, we are proposing that a new partnership be explored with provincial regulators, whereby the RCMP would match resources on a dollar for dollar basis to create a national and integrated approach to securities fraud in Canada, with particular emphasis on the high-tech securities frauds referred to above. Some of the provincial securities commissions have expressed support for this vision. The Ontario Securities Commission (OCS) recently announced that they are working with us and proceeding to build an integrated intelligence unit made up of RCMP officers matched with OSC investigators.

Our proposal includes some significant cost estimates and although we are poised to make our move, it will remain to be seen if we will be successful in building a truly national and effective enforcement team. However, I wish to leave you with one last thought.

---

[14] "Stock Fraud for the 21st Century" *The Globe and Mail*, Toronto, August 4, 2000, at A14.

[15] *Supra* note 8.

VIII. CONSIDER WHAT IS AT RISK

It is reported that the baby boomers are planning their retirement and investing an unprecedented proportion of their net worth. It is also reported that the largest growing users of the Internet are those persons aged over fifty. When we consider these two single facts in unison, I would suggest that one of the most significant crime trends for the next few years will be securities frauds of unprecedented proportions, and they will be directed at our elders. Now, think of your own personal retirement and how important it is to you that your choice of mutual fund is not artificially over-inflated.

Your own retirement plan may be at risk ...