TALES FROM THE PAST: HOW FRAUD INVESTIGATION HAS CHANGED AND NOT CHANGED

This session offers a look from 1982 to 2012 at how fraud investigations have changed, and not changed, given changes in technology, our paperless society, the Canada Sedona principles and now cloud computing. The background looks at historical examples in "the good old days," while the last three-fourths of the presentation focuses on current examples of how major fraud investigations now need to include a multitalented team of lawyers, accountants, IT professionals, data analytic professionals, and others. A relatively current case is included.

JAMES (JIM) BLATCHFORD, CFE, CMA, FCMA, CFI
Partner Advisory Services
MNP LLP
Vancouver, BC

James Blatchford is a partner in MNP's Investigative and Forensic Services practice in Vancouver. Blatchford draws on more than 38 years of experience, first in policing, followed by his career as a forensic accountant to help clients in the corporate, not-for-profit, and government sectors, including First Nations, protect their organizations and resolve fraud, other misconduct, and dispute issues. Blatchford's broad-based experience includes fraud investigations, litigation support, internal control reviews, due diligence, and regulatory compliance reviews. Blatchford has appeared before various levels of court as an expert in forensic accounting for criminal and civil cases.

NOTES

A Short History on Fraud

Anthropologists, historians, Darwin, and yes even Hollywood tell us that in the earliest of times, there was survival of the fittest, and the strong simply took from the weak. The spectrum within which this most likely occurred would be, on one hand, between two individuals (David versus Goliath) and, on the other hand, between civilizations (the rise of the Roman Empire).

Over time, legal codes developed. One of the earliest known codes was of Ur-Nammu in approximately 2100 BC. The laws were structured to indicate the crime and then the related punishment, which included fines and death sentences.

Fast forward to 1760 BC when the Code of Hammurabi of Ancient Babylon was institutionalized. The Code of Hammurabi is one of the most complete ancient legal codes available to us today, and through 282 laws was committed to protecting the weak from being brutalized by the strong. Again, punishment consisted of principally of fines but often also death.

Interestingly, the Code of Hammurabi has one of the first references to fraud:

> *If a herdsman, to whose care cattle or sheep have been entrusted, be guilty of fraud and make false returns of the natural increase, or sell them for money, then shall he be convicted and pay the owner ten times the loss.*

Fast forward several millennia; as civilization spread, so did commerce, so did the law, and so did fraud. There are accounts of fraud in its many forms throughout the historical records of great civilizations into medieval times.

TALES FROM THE PAST

NOTES

As we learn from the Bible, fraud has been evident from the dawn of creation. Remember the story of Adam and Eve and the apple–and the misrepresentations by the snake! And identity theft was evident as well before the birth of Christ, as recounted in the story of Esau. Esau was the eldest son of Isaac and, while out hunting, his younger twin brother Jacob disguised himself as Esau, brought food to their father, and received Isaac's blessing.

Fast forward once more, and as attributed to Pliny the Elder (AD 23 to AD 79), an author, naturalist, natural philosopher, naval and army commander in the early Roman Empire, as well as personal friend of the emperor Vespasian:

> *It is the natural propensity of man to falsify and corrupt everything.*

Even more recently, a former Attorney General stated:

> *Fraud and deceit abound these days more than in former times.*

That Attorney General was none other than Sir Edward Coke, an English Jurist and Member of Parliament, Attorney General to Queen Elizabeth 1, in 1602. Sir Edward is more famous for his prosecution of Sir Walter Raleigh and the Gun Powder Conspiracy.

This leads us to consider how fraud has changed through the ages and how it might change in the future. In my view, the changes over the millennia are characterized as follows:

- Communication—from simple dialogue to mass communication through the Internet
- Range—from contact among local tribesmen to today's global reach of humanity
- Complexity—from very simple misrepresentations to sophisticated schemes

NOTES

While there have been vast changes in communication, range, and complexity, fraud persists. And through this persistence, fraud investigators have had to broaden their knowledge, skills, and expertise to combat fraud. The remainder of this presentation focuses on the period from the early 1980s to the present, with particular emphasis on the handling of evidence during fraud investigations. While many things have changed, some underlying concepts have persisted, much like fraud itself.

Fraud over the Past 3.3 Decades

An index would have the following subtitles:

- 1980s—The Way We Were
- 1990s—The Way We Were Going
- 2000s—Everyone Is Doing It
- 2010s—The Way We Are

In the early 1980s, the author was a (much younger) constable in the RCMP Commercial Crime Section in Vancouver. Much like the Mounties famed Musical Ride, when there was a fraud investigation in progress and a search to be conducted, we "mounted up" in five-ton trucks and charged off in cavalry formation to the suspect business or other location of the search. Everything, and I mean every bit of paper, was seized.

Immediately thereafter, not only junior Constables, but veteran Sergeants and Staff-Sergeants then got to know the SOP Numbering Stamp, and literally thousands of work-hours were spent stamping a unique number on each document. The closest Hollywood ever got to mimicking this stamping process was in the movie *The Producers* where Leopold Bloom led about two dozen accountants in hitting the buttons on adding machines. In any event, the handling of documents in that day and age was "seize

everything, ignore nothing, stamp everything, and smoke break is at 9 a.m., 10 a.m., 11 a.m. …"

In the 1990s, fraud investigators were introduced to technology in the form of document-processing packages. One particular package was "Supertext." These packages were a new tool in the fraud fighter's toolkit.

The stated advantages were that documents would be better organized, controlled, and searched, all the while preserving the chain of custody as there was supposed to be less handling of the original documents. Fraud investigators' time reverted to focusing on the investigation, while clerical staff supervised by the "Constable in Charge of Exhibits" dealt with the document handling and processing.

There were limitations soon learned by fraud investigators, in that the process was still remarkably slow, and there was still "mounds" of paper to process. If anything, there was more document handling. There was still the question of what to seize—did the documentation have evidentiary value or was the process compromised by the scanning of irrelevant documents.

An even greater dilemma was the advent through legal precedence of disclosure. Was disclosure to be made via photocopy, or would electronic copies be provided? Could defense counsel have access to the originals, or was access limited to Supertext alone? And defense counsel played the game, stating that they lacked the "technology" to review the documents, or lacked the "resources" to deal with all of the scanning, or ultimately, the courts lacked the "technology" to deal with the electronic evidence in that venue. There were circumstances where the RCMP held

NOTES

NOTES

training sessions for defense counsel and judges so they could understand Supertext, its advantages and limitations.

By way of example, the RCMP CCS conducted an investigation of a mortgage corporation whose principals were accused of fraud against investors (and borrowers). The fraud was thought to amount to $350 million of "investor funds" managed over a five-year period. The underlying accusation was of a "Ponzi-like" scheme where returns of 28 percent were offered to investors when "traditional returns" were below 6 percent.

In the investigation, investigators seized "everything" from the company. There was additional document evidence in the form of reports to provincial regulators, and documents from investors. The investigation was subsequently refocused on six recent mortgage loans, which had been granted just days and weeks before the mortgage company's license was suspended by the regulator, and the receipt of "new investor funds" in that period.

With a growing number of documents as potential evidence, the RCMP hired a team of clerks with instructions to "start scanning." Later as the investigation progressed, it was realized that a major error had been made from the start, in that the classification of document type became problematic for investigators and forensic accountants. That is, the search criteria for "Cheque," "cheque," "Chq," and "chq" produced a different selection of scanned documents. Similar issues arose with pluralization (i.e., "Cheques") as well as with originals versus photocopies. Both investigators and forensic accountants worried that critical documents were missed in the process, so there was a myriad of cross-checks and other confirmations.

NOTES

It became evident very quickly that the at the initial stages of later investigations, the criteria for the indexing and classification of the seized documents was extremely critical to the efficient and effective examination and analysis of what had become electronic evidence. The limitations of the use of technology in fraud investigations led some investigators to revert to hands-on document management.

Into the new century, the 2000s brought on the "Digital Revolution" with:

- The paperless office
- Internet and intranet
- Email
- Facebook, Twitter, LinkedIn, Skype
- Electronic banking and funds transfers
- Electronic document registration (at land titles, courts, etc.)
- Electronic document storage and transfer

So with the digital revolution came search and seizure of evidence found in traditional file cabinets and desks, briefcases and storage lockers, but as well as in new forms of electronic data storage. We now have servers and other storage systems, desktop and laptop computers (and related paraphernalia), iPhones, BlackBerrys, Androids, iPads, digital cameras, and so on. Floppy discs gave way to smaller discs, which in turn gave way to thumb drives. The age of "electronic discovery" has been thrust upon us.

In the 2000s, we were introduced to the Sedona Principles, and more importantly for Canadian fraud investigators, the Sedona Canada Principles. There are some critical differences between the U.S. and Canada principles, particularly where in the United States it is based on a request for specific documents, whereas in Canada there is

NOTES

a legal duty to produce all potentially relevant documents by all parties. The presentation will include a short review of the key Sedona Canada Principles.

Needless to say, electronic discovery requires caution from fraud investigators, as there are many legal, constitutional, security, and personal privacy issues that yet need to be resolved, particularly in the legal context. However, the explosive growth in electronic data is frankly overwhelming because of the increasing relevance of email, voice mail, texting, social networking, cell-phone technology (particularly voice- and video-capture).

It is estimated that more than 93 percent of all business documents are now in electronic form, and with over 35 percent of corporate communication never reaching paper, the importance of electronic evidence cannot be overstated. Obviously, retention and storage implications are also very relevant.

There are a myriad of new considerations for fraud investigators:

- Nature of the investigation
- Who has ownership rights of the data
- Beginning the investigation or filling in the gaps
- What role is being played—securing evidence for trial or as part of standard regulatory reporting
- Does the target have its own IT department, systems administrator, or is IT support outsourced—considerations for fraud investigators include whether or not there are sophisticated system audits, regular system back-up, and data storage, including off-shore data retention, not to mention "cloud computing"
- Viruses, worms—will the examination of seized data by fraud investigators bring along its own problems
- Costs of recovery of data—who bears the cost

- Relevancy of data—who decides what is relevant
- Solicitor-client privilege, privacy legislation, copyright
- Pornographic material
- Security over sensitive data such as trade secrets, market data, and so on

Each of these questions will be discussed in modest more detail during the presentation. Then, a relatively current real-life example of the issues of electronic discovery and document handling in the 2010s will be presented.

Case Example

The matter involved a commercial litigation where the parties were cross-suing each other, one for $5 million for failure to pay for product delivered, the other for $7 million for misrepresentations on product technology and capabilities. In the course of discovery, one party declared what evidence they considered to be relevant from their accounting database, preparing schedules that they expected their adversary to accept as fact without full disclosure or access to the database. As the litigation proceeded, additional allegations of fraudulent misrepresentation arose from both parties. Ultimately our client, through legal counsel, sought and was granted an Order for the Examination for Discovery of one party's head of IT, and from that examination, further court orders were granted, which resulted in the disclosure of 1 tetra-byte of data, the equivalent of paper which would fill several five-ton trucks.

The subsequent analysis of this data by forensic accountants and data analytics specialists confirmed that there had been no misrepresentations on the part of our client vis-à-vis the technology and capabilities of our client's products, but rather the issues facing the other party were a result of obsolescence over a relatively short period

NOTES

of time of the product purchased. Our client was awarded their $5 million as claimed while the allegations of fraudulent misrepresentation and damages of $7 million were dismissed.

Conclusion

The final message is that while frauds (and other litigious matters) are becoming more sophisticated, and technology becomes more sophisticated, fraud investigators need to become more sophisticated as well. Certainly in larger cases, the fraud investigation team now needs to include data extraction and analytics specialists in addition to investigators, accountants, lawyers, and computer forensic specialists. At the same time, traditional investigative knowledge, skills, and expertise must remain pertinent, as frauds will continue as they have from the dawn of time.

NOTES