"Tales from the Past"

Association of Certified Fraud Examiners - 2013 Canadian Fraud Conference

Date: September 9, 2013

Presented by: James P. (Jim) Blatchford, MBA, CMA, FCMA, CFE, CFI
Partner, Investigative & Forensic Services, Vancouver
Tales from the Crypt – Changes to the Handling of Evidence Gathering from 1980s to Present

- 1980s – The Way We Were
- 1990s – The Way We Were Going
- 2000s – Everyone Is Doing It
- 2010s – The Way We Are
A Short History on Fraud

As we learn from the Holy Bible, fraud has been evident from the dawn of creation

• Adam, Eve and the apple - misrepresentations by the snake

• Some current scams are just “reinventions” - an example of “identify theft” – the story of Esau, the eldest son of Isaac and older twin brother of Jacob. While Esau hunted, Jacob disguised himself as Esau, brought food to their father, and received his blessing.
A Short History on 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.”

~ Hamurabi’s Code of Laws of Ancient Babylon [circa 1727 to 1780 BC, which incidentally predates the Hebrew 10 Commandments by nearly 500 years]
A Short History on Fraud

Some more recent quotes:

“IT is the natural propensity of man to falsify and corrupt everything.”
A Short History on Fraud

Some more recent quotes:

“It is the natural propensity of man to falsify and corrupt everything.”

~ attributed to Pliny the Elder, AD 23 to AD 79
A Short History on Fraud

Some more recent quotes:

“Fraud and deceit abound these days more than in former times”
A Short History on Fraud

Some more recent quotes:

“Fraud and deceit abound these days more than in former times”

~ Sir Edward Coke – 1602
English Jurist and Member of Parliament
Attorney General to Queen Elizabeth
Prosecuted Walter Raleigh and Gun Powder Conspirators
How Has Fraud Changed Over Time

This leads us to consider how fraud has changed through the ages and how might it 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 and social media

• Range – from contact amongst local tribesmen to today’s global reach of humanity

• Complexity – from very simple misrepresentations to sophisticated schemes
Tales from the Crypt – The 1980s
Tales from the Crypt – The 1980s
Tales from the Crypt – The 1980s
Tales from the Crypt – The 1980s
Tales from the Crypt – The 1980s
Tales from the Crypt – The 1980s
Tales from the Crypt – The 1990s

The Introduction of Technology to Fraud Investigations

• "Supertext"

• Stated Advantages
  ➢ Organization of documents
  ➢ Document control
  ➢ Chain of custody preserved

• Fraud investigators' time focusing on investigation, while clerical staff primarily dealt with document handling
Tales from the Crypt – The 1990s
Tales from the Crypt – The 1990s

• Limitations for fraud investigators

• Slow – still dealing with paper; equal amount of handling

• What to seize? – relevancy of documents as to their evidentiary value; scanning of irrelevant documents?

• Disclosure process – hardcopy or electronic?
  ➢ Defense counsel "played the game"
    ▪ "accused lacked resources" to defend
    ▪ "counsel lacked technology" to review documents
    ▪ "courts lacked technology" to hear the evidence
Tales from the Crypt – The 1990s

Case 1 – Mortgage Corporation

• BC private mortgage company; high public exposure

• $350 million in "investor funds" over about 5 year period

• Underlying it all – "Ponzie-like" scheme; advertising 28% return to investors, when "traditional" returns below 6%

• 100+ loans to both individuals and commercial projects prior to concerns raised to regulators and police

• Some "victims" were in fact "benefactors" of the scheme
Tales from the Crypt – The 1990s

Police Investigation

• Seize "everything" from company

• Other document evidence – i.e. reports to provincial regulators

• Eventually – focus on 6 recent mortgage loans, specifically the handling of "new investor funds" just prior to suspension of business by regulators

• "Let's start scanning" – hired a team of clerks
Tales from the Crypt – The 1990s

Limitations for police investigators and forensic accountants

• Search criteria very specific
  - "Cheque", "cheque", "Check", "check", "Chq", "chq" produced different selection of scanned documents
  - Same with pluralization – i.e. "Cheques", …

• Became evident that setting out the criteria at the initial stages of the investigation for indexing and organization of the seized documents was extremely critical to efficient examination and analysis
2000s – Everyone Is Doing It

However, in the early 2000s, for some individuals at least, the limitations of the use of technology in fraud investigations led them to revert to hands-on document searching and handling.
2000s – Everyone Is Doing It
2000s – Everyone Is Doing It
2000s – Everyone Is Doing It
2000s – Everyone Is Doing It

HIS LORDSHIP...

Conrad Black is charged with mail and wire fraud, money laundering, obstruction of justice, racketeering and tax violations.
Tales from the Crypt – The 2000s

Actually, the 2000s brought on the "Digital Revolution" 

- The "paperless office"
- Internet and Intranets
- Email
- "Facebook" / "Twitter" / "LinkedIn" / "Skype"
- Electronic banking and funds transfers
- Electronic document registration at LTO, Courts
- Electronic document storage
- Electronic document transfer
Tales from the Crypt – The 2000s

So, with the "Digital Revolution" comes "evidence" found in:

• File cabinets, desks, briefcases, storage lockers, … &
• Servers and other storage systems
• Desktop and laptop computers
• iPhones, Blackberrys, Android devices
• iPads, flashdrives, digital cameras, …

Thus: Electronic Discovery
Electronic discovery

• Electronic discovery:
  • What is it; … what form does it take; … why is it important?
  • Differentiating: USA vs. Canada
  • The Sedona Canada Principles
  • How electronic documents differ from paper documents?
  • The key steps to electronic discovery
  • Practical aspects of e-Discovery
  • Case Studies
Electronic discovery: A definition

Electronic discovery (also known as E-discovery) refers to any process in which electronic data and information is sought, located, secured and searched with the intention of using it as evidence in civil and/or criminal litigation, or in regulatory processes.
Electronic discovery: Where is it found?

Examples of the different types of data included in electronic discovery are:

- Files residing on laptops, office PC’s, network servers, floppy disks, PDA’s, BlackBerry’s, iPhones, other smart phones, CD & DVD-ROM’s, iPODs, iPADS, …

- Back up tapes, flash sticks, memory cards, 3rd party storage systems, …
Electronic discovery: What form does it take?

Examples of the different types of data included in electronic discovery are:

- Microsoft office files (i.e. Word, Excel, etc.), PowerPoint presentations, accounting databases, …

- Voicemails, e-mail, instant messaging, …

- Photos, Social Network site entries, …
Electronic discovery: What form does it take?

All of this digital content generates metadata as it is forwarded, downloaded, archived, copied or moved which can also become part of discovery in the proceedings.
Electronic discovery: Who here today does it impact?

- Fraud investigators and forensic accountants
- Internal auditors
- Regulatory examiners
- System administrators and IT managers
- Corporate executives and managers
- Essentially, anyone whose hands touch digital media, data, electronic documents, …
Differentiating: Canada versus USA

In Canada the law on what is and what is not *discoverable*, as well as the laws on *privacy* are far more rigid than in USA

- In the USA, where e-Discovery became prevalent, the production of potentially relevant documents comes only in response to a *request for specific documents*

- In Canada there is a *duty* on each party to produce potentially relevant documents
The Sedona Canada Principles

There was a growing recognition throughout Canada that electronically stored information poses new problems and complications for litigants, their counsel and the judiciary, therefore, the guidelines had to be at least National

Misconception was that electronic discovery issues were mainly applicable to big law firms with large documents cases – but electronically stored information has rapidly become a feature of even the most routine of criminal and regulatory investigations, as well as civil cases, including shareholder, matrimonial, and estate disputes.
The Sedona Canada Principles

Principle 1:
Electronically stored information is discoverable.
The Sedona Canada Principles

Principle 2:

In any proceeding, the parties should ensure that steps taken in the discovery process are proportionate, taking into account:

i. the nature and scope of the litigation;
ii. the relevance of the available stored information/data;
iii. its importance to the court’s adjudication; and
iv. the costs, burden and delay that may be imposed on the parties to deal with electronically stored information.
The Sedona Canada Principles

Principle 3:

As soon as litigation is reasonably anticipated, parties must consider their obligation to take reasonable and good faith steps to preserve potentially relevant electronically stored information.
The Sedona Canada Principles

Principle 4:

Counsel and parties should meet and confer as soon as practicable, and on an ongoing basis, regarding the identification, preservation, collection, review and production of electronically stored information.
The Sedona Canada Principles

Principle 5:

The parties should be prepared to produce relevant electronically stored information that is reasonably accessible in terms of cost and burden.
The Sedona Canada Principles

Principle 6:

A party should not be required, absent agreement or a court order based on demonstrated need and relevance, to search for or collect deleted or residual electronically stored information.
The Sedona Canada Principles

Principle 7:
A party may satisfy its obligation to preserve, collect, review and produce electronically stored information in good faith by using electronic tools and processes such as data sampling, searching or by using selection criteria to collect potentially relevant electronically stored information.
The Sedona Canada Principles

Principle 8:

Parties should agree as early as possible in the litigation process on the format in which electronically stored information will be produced. Parties should also agree on the format, content and organization of information to be exchanged in any required list of documents as part of the discovery process.
The Sedona Canada Principles

Principle 9:
During the discovery process parties should agree to or, if necessary, seek judicial direction on measures to protect privileges, privacy, trade secrets and other confidential information relating to the production of electronic documents and data.
The Sedona Canada Principles

Principle 10:
During the discovery process, parties should anticipate and respect the rules of the forum in which the litigation takes place, while appreciating the impact any decisions may have in related actions in other forums.
The Sedona Canada Principles

Principle 11:

Sanctions should be considered by the court where a party will be materially prejudiced by another party’s failure to meet any obligation to preserve, collect, review or produce electronically stored information. The party in default may avoid sanctions if it demonstrates the failure was not intentional or reckless.
The Sedona Canada Principles

Principle 12:

The reasonable costs of preserving, collecting and reviewing electronically stored information will generally be borne by the party producing it. In limited circumstances, it may be appropriate for the parties to arrive at a different allocation of costs on an interim basis, by either agreement or court order.

Copyright © 2008, The Sedona Conference ®. Reprinted courtesy of The Sedona Conference ®
Electronic discovery: What is it?

- Electronic discovery can be carried out offline, on a computer or on a network.

- Court-ordered, government sanctioned, and/or agreement between parties for IT Forensics (for the purpose of obtaining critical evidence) is also a form of electronic discovery.
Electronic discovery: What is it?

Electronic discovery is a rapidly evolving field that goes far beyond mere technology – it gives rise to a variety of legal, constitutional, political, security, and personal privacy issues, with many of these issues yet to be resolved.
Why is it important?

- Explosive growth in electronic data
  - 93% of business documents are electronic
  - 35% of corporate communication never reach paper

- Ever-increasing relevance of e-mail, v-mail, texting, social networking, cell-phone photography and video-capture, ...

- Retention and storage implications
Dealing with volume can be a challenge

- 1 Gigabyte = 50,000 pages or 20 boxes
- 100 Gigabytes = 5,000,000 or 2000 boxes
- 1 Terabyte = 50,000,000 or 20,000 boxes or 50,000 trees made into paper and printed
- Library of Congress = 10 Terabytes
How electronic documents differ from paper documents?

• Large **volume** and **ease** of duplication

• **Persistence** – Electronic documents are hard to dispose of

• Electronic documents are **attached** to tracking information – *meta data*
How electronic documents differ from paper documents – continued?

- Electronic documents are often updated automatically
- Electronic data often needs a software program and/or hardware which may be obsolete
- Electronic documents are searchable and may be dispersed in many locations
The keys steps to electronic discovery

1. Strategize
2. Collect data
3. Prepare data
4. Review data
5. Produce data

Litigation
Strategize

- Evaluate the preservation obligation (suspend any data deletion)
- Anticipate the scope of e-Discovery (relevancy; privilege; proprietary; privacy)
- Strategize the logistics of e-Discovery (internal vs. external assistance)
- Negotiate e-Discovery with the opposing side
Collect Data

- Multiple sources; multiple locations
- Maintaining data integrity (spoilage)
- Chain of custody – data is evidence
- Data collection efficiency
- Data types and collection costs

Questions
Summary Thoughts

“There continues to be a misconception that e-discovery issues are mainly applicable to big law firm, large document cases. Electronically stored information is rapidly becoming a feature of even the most routine of … cases”

- Justice Colin Campbell, Superior Court of Justice, Toronto, Ontario, in Foreword to The Sedona Principles Canadian Edition

“More than globalization or demographic shifts, e-Discovery is the area lawyers feel will have the biggest impact on the practice of law over the next five years …”

- Helen Burnett, Canadian Lawyer Magazine Inc., March 2008
Considerations for Investigators

• What is the nature of investigation or examination?
  ➢ Does the party have any “ownership” rights to the electronic data (i.e. financial institution, accounting firm, …)?
  ➢ Is a Court Order/Regulatory Order feasible, and/or warranted?
  ➢ Solicitor-client privilege?

• Stage of Investigation?
  ➢ Beginning (looking for “all”), or at later stages (“filling in the gaps”) What is the interest of third parties such as police and/or regulators?
Considerations for Investigators

What is the “role” being played >>> securing evidence for investigation proceedings, or securing, analyzing, and reporting on electronic evidence as part of standard regulatory reporting?

- Chain of custody
- Should additional copies of the data be created?
- Security – what happens if electronic data is “lost”? 
Considerations for Investigators

Is the organization to be discovered a “significant” entity, that has its own IT Department, systems administrator, or is IT outsourced?

➢ Any requirements for system audits?
➢ How is daily computer back-up handled?
➢ What about off-shore data processing and storage?
Considerations for Investigators

• Is there any chance that the target electronic evidence would have any viruses, worms, etc.
  ➢ Have to consider “de-worming” the data to avoid infecting the analytical computer equipment

• Costs?
  ➢ What costs does your senior administrators want to bear?
  ➢ What costs are recoverable?

• Relevancy?
  ➢ Who decides what is relevant?
Considerations for Investigators

• Is any of the target electronic evidence subject to solicitor-client privilege, or privacy legislation, or copyright?

• What about pornographic material?

• What about sensitive data such as trade secrets, market size, cost structure, etc.?
Considerations for Investigators

Principle 3: “Counsel and parties should meet and confer as soon as practicable and on an ongoing basis, regarding the identification, preservation, collection, review and production of electronically stored information”

➢ What do you do in circumstances where allegations of fraud are made, but not confirmed without access to the electronic information?

➢ What do you do where you do not want the accused to know that an investigation is underway?
Considerations for Internal Auditors & IT

• What electronic data is **collected and stored** by your organization in the normal course of its “business”?

• What **litigious matters** is your organization likely to be subject to?

• What is overall **corporate policy**?
Considerations for Internal Auditors & IT

What is the connection between the litigious matters and the electronic data?

- What are the key databases and how do they integrate?
- What are the electronic data retention policies, and practices?
- What electronic hardware is “out there” within the organization?

Are the organization’s IT systems “robust” enough?

- Is any part of the IT system subject to independent audit? How often?
- Internal or external audit? Breadth of IT systems audit?
Considerations for Internal Auditors & IT

What are the **organization’s policies** with respect to **personal use** of the **organization’s computer equipment**, iPhones, Blackberry, and other PDA devices?

- Do **employees know** what the policies are?
- How often are the policies **reviewed** by employees?
- What **form of acknowledgement** do employees give?
Considerations for Internal Auditors & IT

What are the organization’s policies with respect to use of personal iPhone/Blackberry/other devices on “company” business?

- Do employees know what the policies are?
- Does an organization want its “systems” discovered in relation to a personal issue of an employee?
Considerations for Executive and Management

Principle 4: “As soon as litigation is reasonably anticipated, parties must consider their obligation to take reasonable and good faith steps to preserve potentially relevant electronically stored information.”

- What resources does the organization have to respond in a relative timely manner to a request for electronic data?

- Can the organization meet your obligations?

- What level of sanctions is the organization prepared to endure for “failure to meet any obligation”?
Case – Who Said *Slide Rules* Were Obsolete

From *Wikipedia*:

The slide rule, also known colloquially as a “slipstick”, is a mechanical analog computer. The slide rule is used primarily for multiplication and division, and also for “scientific” functions such as roots, logarithms and trigonometry, but does not generally perform addition or subtraction. … The use of slide rules continued to grow through the 1950s and 1960s even as digital computing devices were being gradually introduced; but around 1974 the electronic scientific calculator made it largely obsolete and most suppliers exited the business.
Case – Who Said *Slide Rules* Were Obsolete
Case – Who Said *Slide Rules* Were Obsolete
Case – Who Said *Slide Rules* Were Obsolete

- Private company, therefore its financial results were not public knowledge
  - Provided the company with market advantage over publicly traded competitors – secrecy of results was sacrosanct

- Operations across Canada, with approximately 120 outlets

- Retail sales of a broad range of goods and services

- 32 databases, integrated within their “Data Warehouse”
Case – Who Said *Slide Rules Were Obsolete*

- Various computer languages; **interface issues** within the “Warehouse”; systems of **various ages**

- Data within different databases **stored** for varying time frames

- Various **levels of management** had different levels of access to data
  - VP Sales and Operations
  - VP Specialty Product Lines
  - Regional, area, and store managers
Case – Who Said *Slide Rules Were Obsolete*

- Allegation by Supplier that a considerable amount owing for capital equipment used for servicing of *Slide rules* > $5m
- Defense by the Company that amounts not owed (1) due to lack of disclosure of technical information during contracting and delivery phase causing loss of sales, and (2) due to lack of timely deliveries of supplies to service *Slide rules* – last 6 years
- Also counterclaim that fraudulent misrepresentations by the Supplier caused reduction in *Slide rule* sales and servicing, + overall sales of other goods > $6 to $8 million
Case – Who Said *Slide Rules Were Obsolete*

E-Discovery Issues

- Company provided **summary financial data** that they unilaterally extracted from the accounting records (general ledger) within Warehouse; **did not include damage quantification per se but letter stating that data supported defense and counterclaim $$$**

- Company personnel said that **no other relevant data available**

- Data only covered approximately **½ of outlets**, as not all outlets had full *Slide rule* sales and servicing operations

- Data produced in **Excel format**, with unrecognizable **vernacular** in headings
Case – Who Said *Slide Rules* Were Obsolete

Response to E-Discovery Issues

- Parties agreed to meeting with Corporate Controller to explain data and headings, operations of outlets with *Slide rule* sales and service operations versus other outlets, and overall structure of Company

- Determined some further details of Data Warehouse and interaction of various electronic database systems

- Learned that Corporate Controller in position for only last 6 months and therefore did not have any knowledge of *Slide rule* sales and servicing; Head of IT around for 12 years and very knowledgeable
Case – Who Said *Slide Rules Were Obsolete*

Response to E-Discovery Issues

- Letter setting out short-comings of data extraction, including lack of clarity, lack of additional relevant data, and unilateral approach

- Requested additional data:
  - All sales of all products from all stores, in CSV format
  - Monthly management sales reports, by store, of *Slide rule* sales and service, in original PDF format as published at the time of distribution, and in CSV format for potential analyses
  - Monthly sales reports, by store, of all products and all product classes, in original PDF produced at time, and in CSV formats
Case – Who Said *Slide Rules* Were Obsolete

Response to E-Discovery Issues

- Requested additional data – cont’d:
  - Schematic of Data Warehouse, with details of when different systems and software were introduced, updated, & modified
  - Map of outlets which sold and serviced *Slide rules*, with details of store openings and closings over last 7 year period
  - E-mails between VP Sales, VP Specialty Products, and Store Managers with respect to monthly, quarterly, and annual results and trends for *Slide rule* sales and servicing, as well as emails between VP Specialty Products and Supplier’s representative
Case – Who Said *Slide Rules Were Obsolete*

Response to E-Discovery Issues

- Included within Affidavit and presented to Court by Supplier’s legal counsel seeking relief to obtain further electronic evidence
  
  - Lack of certainty of what really was available resulted in Court awarding Supplier’s legal counsel right to have “discovery” of Head of IT by forensic accountant and technical systems expert

  - Also, “discovery” of employee who extracted data for Corporate Controller
Case – Who Said *Slide Rules* Were Obsolete

Results of Additional E-Discovery

- Greater general understanding of 32 databases within Company’s data warehouse
- Clear understanding of how certain of the databases fed information from retail outlets to accounting records
- Clear understanding of management reports generated annually, quarterly, and monthly for benefit of VP Sales, VP Specialty Products, and Store Managers
- Clear understanding that each item sold, including those for *Slide rules*, had a unique data record
Case – Who Said *Slide Rules* Were Obsolete

Results of Additional E-Discovery

- Request for data in CSV format for each sale of every item sold over past 7 years, by date and time, for all 120 stores
- Request for data in PDF format for monthly management reports on sales of *Slide rules* in $$$ and quantities
- Request for data in PDF format for monthly income statements by store, for 120 stores
- Request for all emails between VP Sales and VP Specialty Products regarding results of sales of *Slide rules* for 7 years, plus emails between VP Specialty Products and Supplier rep
Case – Who Said *Slide Rules Were Obsolete*

Response by Company

- Sought relief from Court that *volume of data* was too great so that *cost* to produce was prohibitive

- Sought relief from Court that *certain data was proprietary* in nature and release of data would potentially *compromise its competitive advantage*

- Sought relief from Court that certain *sub-section of data was outside of claims of Suppliers* (albeit that it was within the scope of the counterclaim by the Company)
Case – Who Said *Slide Rules* Were Obsolete

**Decision of the Court**

- Sought relief from Court that volume of data was too great so that cost to produce was prohibitive
  - **Supplier agreed to pay for cost of recovery**
- Sought relief from Court that certain data was proprietary in nature and release of data would potentially compromise its competitive advantage
  - **Supplier was subject to Order of Confidentiality**
- Sought relief from Court that certain sub-section of data was outside of claims of Suppliers
  - **Data was required to defend counterclaim re: lost sales**
Case – Who Said *Slide Rules Were Obsolete*

Results of Additional E-Discovery

- Company produced 1 terabyte of data representing all transactions of all products in approximately 60 outlets with sales of *Slide rules* >> both sales and servicing transactions
- Company changed its pleadings – eliminated loss of sales of all products due to loss of sales of *Slide rules*
- Company produced PDF version of monthly income statements for 60 outlets – indicated that they would produce CSV version
- Company maintained that *emails were not retained* beyond 45 days – remained a point of contention between lawyers
Case – Who Said *Slide Rules Were Obsolete*

Investigation and Analyses - Sales

- **Industry statistics** obtained from national association of manufacturers of *Slide rules*

- Charted sales by month of *Slide rules* over 7 year period, in terms of $$$ and quantities across all manufacturers

- Extracted sales details of each *Slide rule* by date, time, and $$$

- Overlaid *Slide rule* sales by Company against industry results
  - Incredibly close match showing gradual then significant decline in sales of *Slide rules* over 7 years period
  - Evidence sales declined due to “obsolescence”
Case – Who Said *Slide Rules Were Obsolete*

**Investigation and Analyses – Servicing**

- Conducted *date and time analyses* across approximately 60 outlets for *servicing of Slide rules*

- For all but 3 outlets, determined that the *only days when revenues not earned for at least 3 transactions involving servicing of Slide rules were Christmas, New Years and Easter Sunday*
  - Evidence that *sufficient supplies on hand* to attend to all requests for same-day servicing – effectively, *only smaller inventory on hand* and not overall deficiency

- Other 3 outlets had other issues that could not be tied to Supplier alone
Case – Who Said *Slide Rules Were Obsolete*

**Sedona Canada Principles**

- Electronic evidence is discoverable
- Supplier’s counsel took appropriate steps through legal system to **seek disclosure of electronic evidence**, and was willing to bear the cost
- Preservation of evidence by Company was important, but questions about their “reasonable” and “good faith” efforts
- Lots of **dialogue** and exchange of letters between Counsel, and finally **appearances before the Courts** to get appropriate orders for production of data and information
Case – Who Said *Slide Rules Were Obsolete*

**Sedona Canada Principles**

- Format of data is important – required both CSV and PDF versions of data, 1\textsuperscript{st} for analysis and 2\textsuperscript{nd} for knowledge of the key personnel in the Company.
- Judicial directions re: confidentiality, privacy.
- Costs of producing the data became secondary issue due to settlement.
  - Supplier accepted a settlement from the Company for approximately $5.25M, excluding costs of litigation.
2013 – Today’s Issues and Foreseeable Future

• Offshore storage

• Proliferation of Data
  • more electronic data has been produced in the last two years than since the computer was invented

• Storage in the “Clouds”
2013 – Today’s Issues and Foreseeable Future

- What evidence are you as fraud investigators looking for;

- What electronic data is relevant, and reasonably accessible (don’t bring the 5-ton);

- Expand the fraud investigation team to include IT and data analytic specialists

- Work with your client and their legal counsel and use familiar tools such as Court Orders
2013 – Today’s Issues and Foreseeable Future
2013 – Today’s Issues and Foreseeable Future

Brian Burke lawsuit: B.C. court grants him permission to sue online

The court ruling, made Tuesday in B.C. Supreme Court, means Burke can now send private messages to 18 anonymous defendants through their online message boards advising them that they are being sued.

Burke’s legal team has contacted the administrators at each of the message boards requesting information on the identity of the defendants.
2013 – Today’s Issues and Foreseeable Future

• Fraud isn’t going anywhere!!!

• Don’t be afraid of technology – USE IT!

• Be creative

• Rely upon your experience, but be prepared to continually look for new team members and their tools, and be ready to adapt to change
Concluding Comments and Your Questions