



**ÆGIS** e-journal

***Addressing threats that affect your bottom line***

Volume 2 Number 7, July 1999

From the case files of

The LUBRINCO Group  
<http://www.lubrinco.com/>

and

Financial Examinations and Evaluations, Inc.  
<http://www.feeinc.com/>

**Due diligence outside North America and Western Europe? Call us!**

**This month's features:**

- 1. Due Diligence — Letter to the Editor**
- 2. OPSEC, Economic Espionage, and Competitive Intelligence — The Rapps on information brokerage**
- 3. Executive Protection — Bait for kidnapping**
- 4. Technical Issues — Am I being bugged?**
- 5. Real Stories from the Field — A simple tale of collections**
- 6. Book and Product Reviews — Federal Evidence, 1999 Courtroom Manual**
- 7. Free-Subscription/Unsubscription/Copyright Information**

## 1. Due Diligence — Letter to the Editor

Most of you have read about Martin R. Frankel's apparent cunning fraud, in which he appears to have stolen \$350,000,000 from various organizations, including the Catholic church. Since all of the participants were sophisticated entities, both knowledgeable and experienced enough to have exercised due diligence in this affair, this fraud should not have worked.

Rather than analyzing the fraud itself, which we may do at some later date, we would like to print the following letter to the editor, which we believe goes to the heart of the case.

28 June, 1999

I read with some interest today's follow-up piece *Fraud Claims Its First Victims Among Insurers*.

Fraud of this type requires two willing parties: The fraudster and the greedy participant. Participants want to do business with the Mr. Frankels of the world because they have a better story than does anyone else, sufficiently appealing to the participants' sense of avarice as to discourage careful – or even superficial – examination.

It should come as no surprise that, for the cost of a phone call to a regulatory agency, or a *few* hours of a financial investigator's time, each of the participants in *this* debacle could have found out that Frankel had been disciplined several times and had lost several licenses. His violations were so flagrant and so numerous that it would have taken little time to uncover the history of transgressions, but several hours to draft the report.

Mr. Frankel will eventually be caught and stand trial. The facilitators should, in a more timely manner, be held accountable for their cupidity and their failure to exercise due diligence.

And what will have been learned from this? In the future we, as financial investigators, will be calling on at least some of your readers, who, even as we write, are shaking their heads in amazement over this incident. Our experience indicates that, believing themselves to be smarter than those co-opted by Mr. Frankel, most will have no interest whatsoever in exercising due diligence in the affairs of their own enterprise.

## **2. OPSEC, Economic Espionage, and Competitive Intelligence — The Rapps on information brokerage**

You can search the net for many articles about one Mr. Edward James Rapp in Colorado. Recently Mr. Rapp had his information brokerage shut down by the Feds. It seems that *TouchTone Information Services*, an information brokerage, was illegally claiming to telephone companies and banks that they were the institution's customers in order to get information on target companies for their clients.

In one instance his client was a wine company that asked for information on another wine company. The Rapps delivered a 4 month history of the long-distance telephone calls of the target company to their client company. The client company then went after each and every one of the target company's customers. Ouch!

Information brokers who move from research into the area of economic espionage provide a service of great value to their clients: The wine company mentioned above could never have acquired their competition's client list by legal means.

It is unfortunately true that many investigations, both in the private sector and the law enforcement sector, involve some sort of deception. However, there is a real risk that, without controls, unscrupulous investigators, whether public or private, may end up performing illegal acts which place their clients at risk.

Stick with licensed private investigators and business intelligence professionals, for whom there is at least some minimal recourse, and make sure their actions don't put *you* at risk.

## **3. Executive Protection — Bait for kidnapping**

Below is an e-mail that a dear friend and a well-recognized international banker received. He forwarded it to us for our (not so) sage comments.

Email begins:

What I am about to reveal to you is NOT one of those famous Nigerian scams you have so well described in your book, *The Offshore Money Book*, on page 190. By the way, I am amongst those who fell victim to the Nigerian scam: I lost \$5,000 plus in late 1980's. I believe that given your extensive contacts and knowledge in the offshore community, you should be better positioned to help or to know someone who might help in this project.

Basically, I have access to over \$USD100 million in cash. These assets belong to a relative, and are in safe keeping in Africa. That is where I went to investigate the asset last week and to assess the situation. The principal brought the asset to country "B" for safety after a major political upheaval in country "H". The assets are genuine/authentic US dollars denominations, not forgery. And they are from legitimate business profits: artisan and organized gold, diamonds, and other commodities dealings. Because many African states are "cash" economies, it is not unusual to find substantial cash in people's homes when it is not stashed overseas; people do not trust local banks/institutions.

I am inspired to suggest to the principal that he consider an offshore financial move for assets protection, privacy and security. Therefore, I have been directed to organize the placement of this asset offshore: Select the right offshore banks to put the assets; select an experienced offshore adviser with superior skills who can design a plan for the principal and set-up offshore parameters legally and on the best possible terms. My principal has close and regular interaction with local government officials in country "B", (the originating country), who will assist in getting the asset out via wire transfer, as well as other means.

The only "problem" is that all the asset, (cash US\$) have stamps on them; a blue-ink distinctive mark on the surface/sides of the bills, put on by a contractor based in the Middle East. The Contractor was hired originally by the principal to protect the asset when fleeing country "H"! The contractor is asking for \$1000,000 to remove the markings on the bills using a special instrument/chemical. The principal has \$500,000 and needs an investor with the balance. The investor will get a commission for the service rendered. The entire operation should take hours/days (to clean the cash) and then about 60 days to complete the transfer to offshore locations. The \$500,000 could be paid directly to the contractor in Arabia and would never reach Africa. I am planning to return to the "originating" nation to monitor the operation.

I would like to work with a bank owner that you know personally and who could assist in this project. We would consider a lasting relationship with such a banker who could assist in executing this operation. To that end, I would like to meet with you for a close door session and hammer out a plan; in the event that you are willing to consider this proposal. I could travel to meet with you as soon as possible.

Thank you for your consideration."

End of email.

(Our thoughtful (or not so) sage 2nd response...(The 1st response was rather blue and unseemly - not fit for print, you know...))

“I have personally worked with African nationals who have amassed large amounts of US currency. It was amassed in the just the manner described in the e-mail and some was from bribes. The “problem” is this blue ink thing. The only blue ink regularly applied to currency is contained in a blue ink bomb that is placed in satchels of cash or armored cars during robberies. When the blue ink bomb detonates it leaves the currency and the perpetrator stained with blue ink. The purpose of the blue ink is to make the currency and the perpetrator easy to spot. However, even if the currency has been soaked in blue ink (or dragged across a lawn, or partially eaten by termites) it is still US Currency, and is still legal tender. The Treasury Department has a division that does nothing but currency reconstruction when currency has been burned, eaten by termites or passed though the digestive system of a dog (all true stories..), and the Treasury will issue a credit to you for that amount of currency that can be reconstructed. It is all done for free without a front fee for dye removal or chemical treatment.

And the rest of the story....

South Africa has recently reported a dramatic rise in business abductions. Foreign businessmen visiting South Africa are being kidnapped and held for ransom. Foreigners are being lured to South Africa with the offer of easy profits. Lures such as commission to aide in the transfer of stolen money, and the offer of pieces of blue paper that are said to be US dollars covered in blue ink or a security dye, are being used to get the victims to come to South Africa, where they are held for ransom.

South Africa already has 20,000 murders per year and now they are expanding into kidnapping. Don't let greed overcome prudence.

#### **4. Technical Issues — Am I being bugged?**

It is relatively uncommon for an individual or company to be the subject of electronic eavesdropping. This rarity is due, to a large extent, to the fact that in order for you to be bugged (a listening device placed in such a way as to allow your conversations to be overheard) or tapped (a listening device placed in such a way as to allow your telephone conversations to be overheard), the listener must have A) access to the place to be bugged or the phone to be tapped, and B) some means or recording or place from which to be listening to the conversation.

These sorts of access involve a tradeoff between time and money, either potentially offering the needed access. Because of this, it is often cheaper and easier to suborn some party to the conversations than to go to the risk of placing a bug or tap, listening to the conversations, and then recovering the bug or tap, eliminating evidence of the activity.

Electronic eavesdropping can be divided into two categories: That done by law enforcement and that done by everyone else.

Law enforcement uses legal taps. On rare occasion, illegal taps are done without department authorization or knowledge. Legal taps, done under court order, involve no access to the phone lines in question. Rather, a computer feed is generated by the telephone company. There is no way to detect this sort of tap. Illegal taps are done by hooking into the lines. Information is then gathered, attributed to an informant, which then allows generation of a court order for a legal tap. Bugging by law enforcement requires access to the site to be bugged, with the bugs hidden appropriately.

Bugs and taps by other than law enforcement may or may not be legal, depending on the jurisdiction. In some jurisdictions, conversations may be overheard if one party consents, and in some jurisdictions it requires consent of both parties.

Assuming access, how are bugs and taps placed? Taps can be radio taps, where a signal containing the conversation is transmitted, and listened-to or recorded by some other party. Radio signals are fairly easy to detect with the proper equipment and some expertise. Taps can also be wired into the system, either going to an amplifier for direct listening, or going into a tape recorder. These are usually detected by physical inspection, although there is equipment available that will indicate some discontinuity in the wiring. In addition, in a PBX system, the telephone can be programmed to also have the conversation appear on another handset.

Ignoring high-tech attacks such as reading vibrating windows with a laser, and not trying to be all-inclusive, bugs can, with certain telephones, be created by making the handset always live, and listened-to somewhere down the line. Alternatively, radio bugs (again, easily detectable) can be planted. As another choice, some version of a baby monitor can be installed, with the signal being carried through the power line to the listening portion of the monitor. Finally, loudspeakers can be easily used as microphones, so that any PA system can be used for eavesdropping by putting an amplifier and headset somewhere in the wiring.

Because of the technical ease of electronic eavesdropping, when discussing anything confidential, there may be an obligation to exercise due diligence in assuring that you are not overheard. This may include, for a corporation, having a room swept for bugs, not having meetings in a room with a PA system, and not allowing telephones in a room where confidential meetings are held.

How do you know if you are the subject of electronic eavesdropping? In general, it is revealed by a swing in luck: Competitors or associates are one step ahead of you, seem to know what you are planning to do before you do it, are underbidding you fractionally, or are bringing out new products just before you do.

A good rule of thumb in this area is “once is coincidence, twice is a conspiracy.” If you suspect you are the subject of electronic eavesdropping you should bring in a professional to deal with the issue. Keep in mind that you should *NOT* call them from a phone that might be tapped or a location you suspect may be bugged: While not-quite amusing, we have received calls from clients saying they thought they were being bugged and when we ask where they are calling from, all we get is an embarrassed silence....

## **5. Real Stories from the Field — A simple tale of collections**

So you grant credit and then someone abuses it and now you have to collect. But from whom and from what?

The work can go from simple to difficult very quickly, but there are a few basic steps to begin with.

A) Document the debt and all of the information you may have on the debtor and go get a judgment. This process varies from state to state so we can't be specific here.

B) Once you have the judgment on a person or a company, send them a letter so you can warn them about what you are going to do: Give them one last chance. This shows good intentions on your part, and their failure to respond shows bad intentions on their part.

C) Pull a credit report and look for employer information. Call the employer and verify employment. If the employer information is not current begin the process of calling each and every one of the creditors and employers, beginning with the most recent first and going to the oldest last. Ask about employment, residential information, telephone numbers and — if you're lucky — bank accounts.

D) If this doesn't work, go to public records and look for lawsuits either in the small claims area or the county courts. Also look to the County Recorder's office for things such as property, tax liens, etc.: Anything that will give you a clue or new information. For example, a fellow I was looking for had vanished. I knew he was near, but I could not find him until ... a Federal Tax Lien was filed against him with his new address.

E) At this time I usually try to use an innocent pretext. I'll knock on the person's door and ask if they have seen an incident — an accident or a yelling dispute in the street and also ask if I can get their work number so I can call them during the day — to make things easier for them. Bingo!

Here and there, pretexts are needed to finesse information about a debtor. (I am using this example to illustrate the difference between illegal methods used by unscrupulous information brokers and investigators). *Never ever* represent that you are with law enforcement, nor should you ever represent to a third party (bank, telephone company, etc.) that you are the debtor in order to get information to which only the debtor should have access.

Pretexting is an important tool of the investigative trade and must be used properly to get the information you need. If you abuse your ability and go over the line you may blow any chance of recovery, *and* you may hurt your client, *and* you may end up before a judge.

F) Use the attorney's expertise to garnish assets and wages you may have found. Some interesting things to garnish that are usually overlooked: Rental and utility deposits, brokerage accounts, stock in privately held companies, ownership in LLC and Partnerships (ownership records can be found at the state level), value in an automobile or a home over the exemption amounts in your state, etc.

G) Last but not least, sometime you have to get their attention. Work with the local Sheriff's Office and / or the U.S. Marshals Office and clean out their homes and offices. This forces one of three events: Payment in full or part, bankruptcy filing, or debtor flight.

## **6. Book and Product Reviews**

*Federal Evidence, 1999 Courtroom Manual*

Professor Weissenburger

Anderson Publishing Co. \$55.00

<http://www.andersonpublishing.com/> 1-800-582-7295

An excellent reference for all of the professionals involved in litigation, or something that might be litigated. Target readers should include: Attorneys, subrogation specialists, private investigators, and all expert witnesses — and even judges as a reference manual.

Anderson Publishing has been a long-standing publisher of legal reference material and have an excellent track record as a reference source.

## **7. Free-Subscription/Unsubscription/Copyright Information**

•• AEGIS e-journal is supported and maintained by voluntary efforts. This publication is owned, published, and copyright © 1999 by The LUBRINCO Group Ltd, Inc. and Financial Examinations and Evaluations, Inc. It is edited jointly by Richard Isaacs (RBIsaacs@lubrinco.com) and L. Burke Files (LBFiles@lubrinco.com).

**The LUBRINCO Group** provides services in three high-threat areas, too specialized to be dealt-with in-house, that can adversely affect domestic and international bottom lines.

- **Protection of trade secrets and intellectual assets.**
  - Anti-economic espionage.
  - OPSEC: The identification and protection of information that would give your competitors and adversaries an advantage.
- **International financial investigations and due diligence consulting.**
  - Location and recovery of missing and hidden assets.
  - Establishing business relationships and strategic partnerships in Central and Eastern Europe, the offshore financial centers, Beijing and Shanghai, Central Asia, and Latin America and the Caribbean.
  - Anti-money laundering and financial fraud requirements under the *International Money Laundering Abatement and Anti-Terrorist Financing Act of 2001* and the *EU Revised Money Laundering Directive of 2001*.
- **Protection of management, staff, and families.**
  - In the high-threat environments of Latin America, Africa, the Mid-East, and Southeast Asia.
  - When traveling and living overseas.
  - When transporting items of substantial value.

LUBRINCO identifies and quantifies threats and vulnerabilities, and their associated risk, then manages the vulnerabilities so you can transfer or live

with the residual risk. We prevent disastrous financial loss to your company, and physical harm to you, your family, and your staff.

For information on **The LUBRINCO Group** and its services, or for the archive of all past issues of ÆGIS e-journal in PDF format, please go to <http://www.lubrinco.com/>.

To sign up for a **complimentary subscription** to ÆGIS e-journal or the ÆGIS e-journal PDF notification list, go to <http://lb.bcentral.com/ex/manage/subscriberprefs?customerid=7768> or send an email to [ejournal@lubrinco.com](mailto:ejournal@lubrinco.com).

To subscribe to our AvantGo channel, go to [http://avantgo.com/channels/\\_add\\_channel.pl?cha\\_id=1773](http://avantgo.com/channels/_add_channel.pl?cha_id=1773)

To be removed from the subscription list, follow the instructions on the mailing you received, or send an e-mail to [ejournal@lubrinco.com](mailto:ejournal@lubrinco.com).

If you know of anyone else who should be receiving ÆGIS e-journal, please send their e-mail address to [ejournal@lubrinco.com](mailto:ejournal@lubrinco.com).

If there is a topic that you would like to know more about, send it to [ejournal@lubrinco.com](mailto:ejournal@lubrinco.com) and the editors will consider it as the topic for an article in an upcoming issue.

If you would like to submit an article for publication in ÆGIS e-journal, send it as an attachment to an e-mail to [ejournal@lubrinco.com](mailto:ejournal@lubrinco.com). Submission of an article certifies that (a) all information in the article is in the public record, or (b) that you are authorized to release any personal or corporate proprietary information contained in the article, and (c) that none of the article has previously been copyrighted. The submission of materials for publication in ÆGIS e-journal constitutes a license to The LUBRINCO Group Ltd, Inc., and/or Financial Examinations and Evaluations, Inc, their assigns, associates, or affiliates, to abridge and/or edit said submission, and to copyright and publish/republish any submitted materials in whatever written and/or electronic form they may choose.

If you would like to go beyond normal fair-use in reproducing articles from this issue of ÆGIS e-journal, you may do so freely as long as appropriate source, copyright, accreditation, and link to the LUBRINCO website is included. This should be in the form

*Article Title*, from the July 1999 ÆGIS e-journal (© 1999 LUBRINCO & FEE), to be found at <http://www.lubrinco.com/>.

ÆGIS e-journal is a forum for the exchange of information, ideas, operating styles, theories, and related topics for corporate managers who make decisions about threats typically outside the expertise available in-house, yet which have the potential to affect their company's domestic and international bottom lines. Nothing appearing in ÆGIS e-journal should be construed as legal advice. The information provided is "general information," not "specific advice."

The solution to any problem is highly dependent upon the precise facts involved. Thus, before making any reliance upon anything said here, you should consult with an appropriately skilled professional. Opinions expressed by contributors are not necessarily endorsed by the publisher, and may be presented to encourage a dialogue among subscribers. The publisher and any re-publisher cannot be held responsible for any loss incurred as a result of the application of any information published in ÆGIS e-journal.

Please be safe, and be smart.