



**ÆGIS** e-journal

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

Volume 5 Number 2, February 2002

From the case files of

The LUBRINCO Group

<http://www.lubrinco.com/>

and

Financial Examinations and Evaluations, Inc.

<http://www.feeinc.com/>

**Concealed assets in fraud, theft, and divorce? Call us!**

**This month's features:**

- 1. Due Diligence — Cooperative marketing fraud**
- 2. OPSEC, Economic Espionage, and Competitive Intelligence — Why you should hire us to do an OPSEC audit, even though you are bigger than we are**
- 3. Executive Protection — Counter-surveillance as an alternative to protection**
- 4. Technical Issues — Stealing from debit cards**
- 5. Real Stories from the Field — A field audit**
- 6. Book and Product Reviews — Practical Handbook for Private Investigations**
- 7. Free-Subscription/Unsubscription/Copyright Information**

## 1. Due Diligence — Cooperative marketing fraud

We never met a fraud we didn't like. This one was not exceptional, but still sort of cute.

A client of ours is involved in the national sales of a commodity item. The product does not differ much from other similar products, nor are the distributors much different from others selling and distributing this or similar products. Because of these factors, the company relies heavily on advertising, which is, of course, the great differentiator.

The advertising is paid for through a cooperative marketing campaign in concert with the manufacturer of the product. The company pays for the advertising, and the manufacturer reimburses a portion or all of the advertising costs. Further, the local managers for the company place most of the advertising for their region, with the understanding that local managers know better which stations will attract the clientele interested in their product. Well – as always in this column – something goes wrong. It seems the advertising agency and one of the local managers were in league with one another to defraud the client.

The advertising agency claimed to have paid for 200 radio ads, but actually ran only 20 and added, with the help of a copy machine, an “0” to the number of ads run and to the total amount of the invoice. The funds for the 180 phantom ads were then split between the local manager and the owner of the advertising agency.

How do you avoid this? Upon request, each radio and TV station will supply an *Affidavit of Performance* that is signed and notarized. While these too can be subject to copier “creation” and alterations, the customer can require that they be sent directly from the station that ran the ads. The FCC also requires both TV and radio stations to maintain a log of everything that is broadcast. A client can simply call any or all of the TV and radio stations that are listed on an invoice and ask for a copy of the log showing the ads that were run. This log is a public document; the station is required to keep it and to make it available to the public.

For printed media the equivalent is a *tear sheet* (the advertisement torn out of the publication) sent to the client along with an “Affidavit of Publication”

## **2. OPSEC, Economic Espionage, and Competitive Intelligence — Why you should hire us to do an OPSEC audit, even though you are bigger than we are**

I recently spent time with a manager of a company that has a genuine commitment to both safety and security. Because of their size and commitment, their security department is, in fact, excellent. Indeed, it is so good that they do outside security consulting and bring in literally hundreds of millions of dollars in security consulting revenues.

I also spent time with someone way down the corporate food chain, and discovered that, as so often happens, they desperately needed an outside audit, which would allow them to see, in a non-threatening way, where policy has gone astray within the corporation.

As an example, while the manager talked about the disposal of documents, at the bottom and middle rungs of the corporate ladder (and, we are willing to guess, even higher), what *really* happens is that papers deemed to be unimportant (by folks not really qualified to make the judgment) are discarded intact. Papers thought to be of potential sensitivity are torn up by hand. Papers believed to be actually sensitive are run through a strip shredder.

In fact, it would appear from our conversations that this excellent company does not actually have an implemented OPSEC program.

We deal mostly with companies that are very large, and they always have security departments that are very much larger than The LUBRINCO Group, and these departments are generally well-run and competent. So why do they hire us? Because while they are *generalists* in corporate security, we are *specialists* in three areas in which it makes no economic sense for most organizations to have extensive staff. These areas are:

- High-risk protective services
- OPSEC consulting and economic espionage investigations
- Due diligence (which we define as anything where you might face liability for negligent actions) consulting and financial investigations

In performing audits for our client companies on existing programs we usually find that most things are being done right. Because we are not there to place blame, when a problem is found, we discuss the problem, not who is causing it, and we generally get co-operation from staff members who know that they can speak with us in confidence, without having to face the ire of a supervisor. When we come in to help establish a new program, we generally

get co-operation because we are there to help, and will then leave, making the staff look better after our departure: While we want the internal program to run successfully, we don't want to do it ourselves, or replace existing staff with our staff.

So if you have an existing program, it behooves you to give us a call as part of your independent audit. And if you need an OPSEC program, we are ready to help you get it going.

### **3. Executive Protection — Counter-surveillance as an alternative to protection**

On a recent trip to Bogota I met with a man who no longer made use of protective agents. His reasoning was that no matter how much he paid his people, the bad guys could pay them more. This is a valid concern, as trust always is an issue (without trust there can be no betrayal), which is why we sometimes get called in for sensitive operations because we are by reputation trustworthy (we vet our people very carefully and on an ongoing basis, and this writer is, literally, an Eagle Scout), as well as because of our capabilities.

Instead, he chose an alternative approach to making himself inaccessible. Rather than having one office he had three, and instead of having one car he had five. Each day he would randomly choose a car, and then randomly choose an office. By having fifteen office/automobile options, rather than one, he believed he had made himself a less-available target, a belief that was confirmed for him by the fact that he had not been kidnapped.

While we are, in fact, delighted that he is safe, and hope this state of grace continues indefinitely, there is a small flaw in his logic. This flaw is the underlying assumption that kidnappings are relatively spur-of-the-moment affairs, and that switching cars and offices will confuse potential kidnappers.

In fact, kidnappers spend a *lot* of time investigating possible targets, choosing the appropriate target from a list of potential candidates, and planning the snatch. Indeed, the selection and planning stage rarely take less than six months, and frequently take more than a year. Thus, for our thus-far lucky subject, the fact that he leaves from one residence to go to one of three offices is not likely to be much of a deterrent.

The very thoroughness of kidnappers could, however, be turned to his advantage if he could assemble at least a small counter-surveillance team that he can trust. Naturally, if you have a problem trusting your protective agents, you will also have a problem trusting your counter-surveillance team, though this is minimized by the fact that they are, by nature, nearly invisible. In the case in question, the team would be responsible not for

protection, but for counter-surveillance. Counter-surveillance generally begins with surveillance: When you notice that you are tripping over others doing the same surveillance as are you, then you know you have a problem which needs to be addressed.

And, of course, even if you *do* have a protective team, counter-surveillance, like intelligence gathering, should be one of its cornerstones. Be aware, however, that counter-surveillance is a skill that comes through training and experience. If your team doesn't have that skill set, call us to talk about getting some training for them.

#### **4. Technical Issues — Stealing from debit cards**

In a sure sign that identity thieves are developing more sophisticated techniques, dozens of debit cardholders from several banks have found that money was improperly withdrawn from their accounts, but that their cards and bank cards never left their wallets!

The thieves, who are still being sought by state and federal law enforcement agents, used devices at non-bank automated teller machines – probably at small markets and convenience stores, authorities say – that skim the information from a card's magnetic stripe and simultaneously record the customer's personal identification number with devices such as a hidden camera or a false cover on a PIN pad.

Fraud feasons are more clever than ever in stealing peoples' card information, particularly their PIN codes, and the rigging of ATMs is a worldwide problem and is more prevalent in the last years.

In the beginning, fraudsters would place a false card reader over the normal slot. They would also use a camera to record the cardholder's PIN. But this technique was far from perfect, because they would have to match each card's information with the correct PIN. The technology was cumbersome, for example, when a card was ejected from a machine, the customer might have noticed that the card was more difficult to remove. Hence the thieves have developed skimming devices that are more elegant in terms of design, so they look like they belong on the ATM.

Fraud feasons now place duplicate PIN pad overlays over actual PIN pads. The device is very thin and within it is a transmitter to record the PIN. So when the cardholder presses down on the PIN pad, both the overlay and the actual PIN pad record the PIN. The transaction goes through, but the cardholder's information is recorded on the false PIN pad and immediately available to the thieves. The duplication of the ATM card with the victim's

accounts numbers and the new PIN is the easy part. The withdrawing of the money is the fun part.

Spokesmen for the banks confirmed that some customers have fallen prey to this scheme and that the companies are working with law enforcement to catch the thieves, who appear to be working as part of a sizable crime ring, and will restore any money stolen from customers. (Warning – that is if you can make the claim stick; it is never easy to get a loss claim to stick with your bank. You will have only a short time, 30 days or less, from when your statement is mailed to make and document the loss claim to the bank.)

The bankers claim to be “aware of some isolated discrepancies” and we are working with law enforcement authorizes in their investigation. We’re working with any customers who may have been affected to resolve the issue as quickly as possible. We regret any inconvenience (loss and time trying to recover the loss) our customers may have experienced.”

## **5. Real Stories from the Field — A field audit**

In the 1983 film *Superman III*, a company discovers that money is being cleverly stolen, and despairs of finding a thief that cunning. Just then they hear a squeal of tires, look out the window, and see Richard Pryor, a junior programmer, arriving in his new, expensive, red, expensive, imported, expensive, sports car. Management considers this to be A Clue.

Companies need to be actively looking for clues, and acting on them when they appear. There are a lot of ways that this is done, from checking regularly to see if there are phantom employees (they tend to get a salary but no benefits), through following procedures know to reduce the opportunity for theft, to watching for anomalous behavior.

As an example, someone mentioned in passing to a company owner that one of his employees in a branch office repair department was spending a lot of time with prostitutes. Since this employee didn’t make enough money to afford to do this, the owner recognized this as A Clue.

He sent in a crew on a Sunday and they went through the books and records, all of which were fine. They counted the inventory, which matched up. Then they actually started opening all the boxes and looking at the inventory.

What they discovered was that the employee had been selling the new parts, and replacing them with old parts.

A significant number of companies go out of business because of employee theft, and any audit that depends entirely on cooked books with no

verification represents a failure to exercise due diligence. It behooves you to be aware of this problem, make an effort to hire screened employees, and work to minimize the effects of dishonest employees who slip through your background checks.

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

*Practical Handbook for Private Investigations*

Rory J. McMahon

CRC Press

<http://www.crcpress.com/> ISBN: 0849302900 1-800-272-7737 \$59.95

It is tough for a private investigator to review a book telling us how to do what it is we already do: One has strongly held opinions on that. It like asking a golf pro if a doodad that helps improve your swing will sell. The answer is always “no it won’t,” yet these things sell in the millions. Well, same problem here. Mr. McMahon is a seasoned veteran on teaching and investigations and any effort on publication in this area is so hard to begin with, it definitely needed good hands, so we did what any person who is honest with themselves actually does: We gave the project to a few people who are not so close to the industry (our interns). Our interns genuinely liked the book for the ideas and the thoughts on the industry. The book covers many of the different fields of a diverse industry in a good summary fashion. It deals with the general facts of the investigative profession and not so much with the art.

It is genuinely difficult to write a book that could deal in detail with everything from Cattle Rustling Investigations to Aircraft Accident investigations, so an author must stay a generalist to remain relevant to all areas. The book takes a reader from no knowledge to a good beginning point for becoming an investigator. All of my interns recommend it as a buy, and it helped some of my interns learn about things I thought everyone already knew, and so I omitted from my training. Thus if you are interested buy it. Audience for book: new PI’s, and people such as attorneys who need to know how to use a PI, and law enforcement to understand how PI’s work.

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

•• AEGIS e-journal is supported and maintained by voluntary efforts. This publication is owned, published, and copyright © 2002 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 2002* and the *EU Revised Money Laundering Directive of 2002*.
- **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 February 2002 ÆGIS e-journal (© 2002 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.