



ÆGIS e-journal

Addressing threats that affect your bottom line

Volume 2 Number 11, November 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 — Identity theft**
- 2. OPSEC, Economic Espionage, and Competitive Intelligence — False claims and their counterclaims**
- 3. Executive Protection — Why you should plan to kidnap your boss**
- 4. Technical Issues – HERF and HERF guns**
- 5. Real Stories from the Field — Land liquidation schemes**
- 6. Book and Product Reviews — Public Records Online**
- 7. Free-Subscription/Unsubscription/Copyright Information**

1. Due Diligence — Identity theft

Last year, for most, the problem of identity theft wasn't even on the radar screen, and now it is all over the place. All someone needs to have is your name, SSN, DOB and some basic additional information such as where you live, or what you drive, etc.... With this information, identity thieves can acquire IDs such as a voter registration card, Social Security card, and other similar non-photo ID Cards. From these documents they begin the process of obtaining government photo IDs such as drivers licenses.

Why do people do this: Why do they steal someone else's ID? It is done because they have screwed up their own lives — or because they are going to screw up the life of the person whose ID they stole. One man in Texas assumed another man's ID **35 years ago** when he was given a dishonorable discharge from the military. The man whose ID was stolen lived in Maryland, and had tried for almost all of the 35 years to make authorities aware that something was wrong. It wasn't until new federal law was passed against ID theft, and over \$400,000 in credit fraud was logged against him, that something was done. The identity thief in Texas is finally in jail awaiting trial.

How do you prevent your ID from being stolen? Shred all documents containing any personal information before they go into your trash. Don't throw out any documents, such as checks or anything else, away from home: Take them home and shred them. Don't use your Social Security number on your drivers license, and don't routinely give out your Social Security number or date of birth. Keep only the minimum of documents in the glove box of your car. Also, check your credit report at least once a year and look for unauthorized inquiries and unknown credit relationships. If these occur, *immediately* contact the credit granting body and the credit reporting agency.

How do you know if the person you are hiring is the person they claim to be? Without doing routine background checks this can be a problem. This was a problem for a series of banks that hired loan officers. It seems a group of criminals applied all over a city as loan officers. Where they were hired they immediately began issuing loans to their criminal associates, and, surprise of surprises, all of the loans went bad. The banks that did not conduct background checks hired the criminals, and suffered losses: Millions are missing, and the banks have no one to blame but themselves.

On the bright side, those banks that did background checks found discrepancies, and did not hire the criminals. Simple cross references

between names, Social Security numbers, addresses, ages and, drivers licenses photos caught the fakes.

2. OPSEC, Economic Espionage, and Competitive Intelligence — False claims and their counterclaims

As citizens, most of us believe that certain institutions should be above the perceived standard of a used car salesman's plaid jacket, tricks and chicanery and puffery (this editor owns a used car lot, so he can say these things). In general most institutions are above this level, but sometimes they not *much* above this level.

In recent months, in a western state, Rock Trust Company sued Paper Trust Company (the names have been changed to protect everyone), accusing them of stealing employees and accounts. Paper Trust responded "We did not steal employees and accounts: They ran from you!"

A defensive investigation of Rock Trust by Paper Trust indicated that Rock Trust's advertisements were so false that puffery as a defense was not available. As an example, Rock Trust had a web-site advertising its services. The web site contained numerous statements about Rock Trust and it's activities that were completely inaccurate — more than could be accounted for through error and even sloppiness:

- It listed the wrong date of founding.
- It had the wrong address for the company, using a much more prestigious address on the web than their true physical address.
- It claimed performance standards that were greater than any other trust company (Paper Trus found out that Rock's principals routinely rounded up performance standards every month (a 3.41 performance standard would become a 3.5 performance standard) so that, the end of the year, their cumulative rounding errors would compound and overstate their performance by 20% a year.
- It alleged that they were the largest trust company in their region. They were not. There were about 20 larger.
- It alleged that the principals of the trust company hosted their own weekly media event on TV, They did not. It had been canceled for a year and a half.
- And further, it stated: "Our reputation and integrity are our most valuable assets."

The Judge issued a summary ruling against Rock Trust Company in favor of Paper Trust Company, requiring Rock to so notify all of its clients, as well as having to recast their advertising and recast their earnings subject to an independent review and audit.

In fact, this being the real world, Rock did not do that. Since they had a subsidiary trust company in another state they folded to their assets into the subsidiary, closed operations of the former parent company, and lived happily ever after.

The lesson to be learned here is no matter what financial institution you have been dealing with, whether it be a trust company, a bank, a brokerage firm, or an insurance company, you can not necessarily believe the representations of the company without an independent third part verification. All items that can not be independently verified by a third party should be taken with a grain of salt.

It is also a lesson in the fact that competitive intelligence can be used as a tool in litigation, and force unseemly disclosures and costly recalls.

3. Executive Protection — Why you should plan to kidnap your boss

If we in the protective services do our jobs properly, nothing bad happens to the folks we are protecting.

When nothing bad happens, two potentially disastrous things can fall out of this good fortune. The first bad thing is that someone can make the decision that protective services should stop, since a lot of money is being spent for no apparent reason. At which point something *really* bad happens.

Second, we, the people providing the protective services, can start to take the job for granted, lowering our level of alertness. This is not unlike a cop who starts to believe that there are high-risk traffic stops and low-risk traffic stops, rather than recognizing the reality that there are high-risk traffic stops and *unknown*-risk traffic stops. At which point something *really* bad happens.

One of the ways to keep alertness at an appropriate level is to look at what is being done from the other side; from the perspective of the bad guy. It is important to think of criminals as risk-averse businessmen, and plan accordingly. This means that before criminals commit their crimes they spend as much time in intelligence gathering and planning as do legitimate businesses. In many cases, we discover that something between six months and a year has been spent choosing a potential target for the crime, investigating the target's situation, watching the target, and planning the

action. As with a legitimate business, detailed records are kept for analysis, and alternative plans are made. In many cases this process is repeated several times until an appropriate target for the crime in question is found.

In order to prevent these crimes from taking place, we ideally want to be able to detect them in the planning stage. An effective way to do this is to plan these crimes ourselves. As we prepare the plans, and investigate the possible ways to commit them, we should become sensitive to others who are doing the same thing.

Thus, if we plan to kidnap our boss, we will have to begin a surveillance of his activities, tracking his travels from home to work and back, and his other travels. Is our surveillance detected? If not, we have a problem, because it means that other, more ill-intentioned, surveillances will also go undetected. If our surveillance is not detected, then the counter-surveillance skills or the protective team definitely need brushing-up.

Are we seeing anyone else doing surveillance? Have we taken counter-surveillance training recently? If we come across someone behaving as suspiciously as are we, then we need to take some appropriate corrective action.

As we continue our surveillance and planning we will discover points of vulnerability. And if we are discovering these, so will a potential real kidnapper. This means that as the weak points are discovered, they must be strengthened. Points of risk are frequently found at those places from which we habitually come and to which we habitually go: We usually have one home and one office, and these are fixed points that cannot be avoided.

As an example, on April 29 1992 the president of Exxon International, Sidney Reso, was kidnapped after a lengthy (four or five months) selection and elimination process. He was snatched when he got out to pick up a newspaper on the ground near the secluded mailbox at the end of his driveway. In Reso's case this was an observable danger spot, as shown by the fact that at one point in the investigation an Exxon security person asked if that was where he was kidnapped (a question which apparently earned him a lengthy interrogation).

If an obvious area of risk is identified yet not made safe, then shame on the protective team, or on those higher up the food-chain who won't let them make it safe. If an obvious area is *not* identified, then shame on the protective team, or on those higher up the food-chain who won't let them work to identify areas of potential danger.

4. Technical Issues — HERF and HERF guns

According to a California engineer who demonstrated a home-brew computer death-ray, with \$500 and a trip to the hardware store saboteurs can build a device capable of remotely disrupting computers, automobiles, medical equipment, and nearly anything else dependent on electronics.

The engineer showed off an unwieldy device constructed from a parabolic reflector, a horn antenna, and two automotive ignition coils, which he aimed at two personal computers about 20 feet away. When an assistant activated the device by connecting it to a car battery, the room filled with a loud buzzing from the PA system and a Power Point presentation on one of the computers flickered and scattered. The other computer instantly dropped out of its screen saver. When the device was switched off, both PCs were frozen, and wouldn't respond to keyboard input.

The effects of High Energy Radio Frequency (HERF) emissions on electronics are well known among engineers, and info-warriors have expressed concern that adversarial nations may someday include computer-killing devices in their arsenals. But small-scale electronic warfare is possible, and even low-budget saboteurs can create viable electronic weapons.

The HERF gun is not particularly high-tech. The device uses technology dating back to Tesla, essentially pushing a 20-megawatt burst of undisciplined radio noise through an antenna. The energy is enough to interfere with sensitive computer components nearby, creating unpredictable results ranging from minor anomalous behavior to complete burnout. Larger HERF guns are capable of crashing computers and disabling automobiles at a range of 100 feet, with a cost as low as \$300.

The computers targeted in the demonstration worked fine after rebooting, and permanent damage is uncommon. "But if that happens to be a computer in a tank, or in a piece of medical equipment, how long does it take to reboot?... By that time you could be dead."

HERF gunning is outside the scope of firewalling but it is an issue to be addressed as a real concern, and a HERF attack might be regarded as a variation in 'denial of service attacks,' as are attacks on firewalls, as well as many computer viruses.

The question of whether HERF guns exist (they do) and, if so, whether they work (they work) is less important in some respects than the fact that several incidents have involved claims by extortionists that convinced the victims to part with money.

What is still conjecture is how many victims have been hit and how much they paid for ‘protection.’ At least one police force would like to know the answers in their area of jurisdiction. As with many incidents of extortion, victims are very reluctant to admit that they have been targeted or that they have paid. One reason for that is that they don’t want to look vulnerable and stupid. Another good reason is that they don’t want to encourage further attacks.

5. Real Stories from the Field — Land liquidation schemes

Tens of thousands of frustrated property owners across the United States and Canada are getting sucked into an explosion of real estate “liquidation” firms. The liquidation firms, in exchange for an advance fee in the area of \$250 to \$1,000, promise to find buyers for un-salable property. With a barrage of sophisticated direct mail and telemarketing solicitations, these firms are telling weary property owners that the up-front charge is a marketing fee needed to cover the cost of promoting the properties on television, radio, a nationwide computer database, mass mailings, ad nauseum. Property owners are assured that their property will be marketed until sold!

The fact is, that in *most* cases, once the fee is collected, the firm is never heard from again. That is called the “No-Pester” guarantee. Once you send them your money, we’ll guarantee they won’t pester you. It leaves the person still holding the property and the loss of hundreds of dollars. These land liquidation promotions have generated complaints in almost all US states and Canadian provinces. Further, a lot of these land liquidation schemes use assurances such as stating they are registered and bonded by state agencies, giving the false impression that they can also provide real estate brokerage services, even though they are not licensed to do so.

These liquidation scams are cruel because they exploit the desperation of property owners who want to sell a piece of land or a property, but have not been able to do so. The land liquidation firms use familiar abuse tactics to get the people to part with their money. Owners of raw land, timeshares, and trailer park lots are particularly susceptible.

These firms are under investigation all across the United States. In Texas, where a woman sent in a \$388 check to a liquidation firm, she was told she would momentarily be receiving a contract in the mail. Of course the contract never arrived. In Oregon, a man sent \$495 via Federal Express to the liquidation firm so he could sell his timeshare. When a contract *was* sent to this man, he refused to sign it because the terms differed substantially

from what was discussed on the phone solicitation. But the company refused to refund the sales fee. A recorded conversation between real estate liquidation sales persons in Idaho got one couple on the hook for a fee of \$695 by stating: "At a price of \$16,000, I am showing that if you keep it at that, I have got between 18 and 20 buyers registered in the computer that we can show it to today." In Arizona, Cease and Desist orders have been issued against seven out-of-state and six in-state real estate liquidation firms. In Alabama, one man sent in \$250 in response to someone offering to sell his property for seven times its actual market value.

Let's face it, this is a typical scheme: Empty promises, sophisticated outreach to potential victims, and demand for advance fee, followed by unresponsiveness. But in these particular cases, the author does not feel particularly charitable toward most of the victims. As in any fraud, you need a perpetrator and a victim. Both of them must be willing participants. In this, as in almost every other case, the perpetrator has hit the greed (and admittedly in some cases the desperation, for which we do feel sympathy) factor on the victim. The victims think they are going to put something over on someone else and unload a worthless piece of real estate.

Some of the companies involved that have received cease and desist orders are:

ADNET Inc., DBA the Advertising Network (Texas);
American Land Liquidators, Inc. (Texas);
Resort Properties Marketing, AKA Resort Nationwide Land Liquidators,
AKA Nationwide Liquidation Services Inc., (Texas);
Prime Property Locators, Inc.(Missouri);
Properties Marketing (Texas);
TRY-VIEW Inc.(Texas);
Universal Land Liquidators Inc., AKA Universal Liquidators, Inc., (Texas).

6. Book and Product Reviews

Public Records Online

Edited by Michael L. Sankey and James R. Flowers, Jr.

Facts on Demand Press \$19.95

<http://www.brbpub.com/> 1-800-929-3811

When they said someone was going to be a desk jockey 20 years ago it was a euphemism for be sent someplace where not much happens. No longer: Not with today's investigator and a computer, the Internet and books like *Public Records Online*. This book has no fluff - just meat. It has resources

for all of this nation's counties, states, and most federal government agencies — all in this one book. It also has a comprehensive list of service providers and private companies that have data for the investigator. If using this book saves you 15 minutes looking for something or someone. then at \$19.95 it has paid for itself. This is an excellent book and a “Must Purchase” recommendation for anyone who is serious about investigative work.

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.

To subscribe to our AvantGo channel, go to 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.

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

If there is a topic that you would like to know more about, send it to 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. 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 November 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.