



ÆGIS e-journal

Addressing threats that affect your bottom line

Volume 2 Number 12, December 1999

From the case files of

The LUBRINCO Group

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

and

Financial Examinations and Evaluations, Inc.

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

Intellectual property being stolen or at risk? Call us!

This month's features:

- 1. Due Diligence — Slumlords: How they make a buck**
- 2. OPSEC, Economic Espionage, and Competitive Intelligence — TEMPEST**
- 3. Executive Protection — Dealing with stalkers**
- 4. Technical Issues – Y2K - Next to the last**
- 5. Real Stories from the Field — Peruvian guano bonds**
- 6. Book and Product Reviews — The Sourcebook**
- 7. Free-Subscription/Unsubscription/Copyright Information**

1. Due Diligence — Slumlords —How they make a buck

We hear so much about slumlords and how they steal property: They get it cheap, they collect rent, and never make any repairs. Ethical issues aside, why would these people do this — if there weren't substantial financial rewards? The fact is, they wouldn't.

The typical slumlord acquires property for little or no money down, probably no more than 10% down on a given property. They typically try to buy a property for between \$15,000.00 and \$20,000.00 per unit, no more. This has to do with cash flow considerations that we will get into later. These properties can be anywhere from a simple four-plex to a large apartment complex that has gone into foreclosure. Either way, there are reasons for a "distressed sale." The distress may be that of the person who wants to get out of the apartment business, or that an insurance company or another lender has foreclosed on the previous owner of the apartment complex and has put the property up for auction: Sale to the highest public bidder. The distress can also be rents that do not support the upkeep of the building under typical, market rate financing conditions, especially where rent control regulations are in place.

In any case, the typical slumlord comes in, and does not argue price: They argue terms. Typically, the terms are for lower than market rate interest and a 30-year time period to repay the rent. Or anything that amortizes as a 30-year note. It may have a 10-year balloon or 15-year balloon: They really don't care past the first five years as long as they can reduce the payment to the lowest amount possible in the first five year time period. The slumlord will then purchase the property. The seller will have little problem with the first one to five payments.

Then the complaints from the buyer begin. These complaints can range from deception on the part of the seller, undisclosed problems, and unknown problems that were not previously disclosed. This editor has seen excuses such as: Undisclosed galvanized pipes; Undisclosed environmental liability from asbestos (one of the newest — and most favored — ones I have seen); Undisclosed structural damage; And a host of other things that would cause some angst if the person were to initiate foreclosure proceedings and then have to sell a piece of damaged merchandise again. A property that they thought was in perfectly good shape when they sold it to the slumlord.

It is this point in time that the slumlord begins making either no payments or only partial payments on the note. He will use a variety of legal tricks,

including stringing out the foreclosure proceedings, counter-claiming for any number of the host of previously alleged defects or undisclosed environmental liabilities, or by claiming that the entire payment had been made but that the owners of the title company have lost them. The purpose here is to realize that the intent of the slumlord is to make little or no payment to the seller or the financier for as long as humanly possible.

The most successful of these I have seen ran three years. The new owner of the property, an attorney, claimed that there was an asbestos problem and that the ceilings of the entire building were filled with what appeared to be asbestos and that it was going to cost 1.1 million dollars to remove. Well, the building was only worth \$3.5 and the bank wasn't crazy about having to invest another \$1.1 million. The bank sat on their thumbs for a year and a half. Finally, they had enough, and unbeknownst to the owner, initiated a testing program on the property. They found out that the ceiling was filled with mica, not asbestos, and immediately initiated foreclosure proceedings.

As the foreclosure date approached, the owner of the property filed for protection under Chapter 11 bankruptcy laws. He forestalled the bankruptcy for another year. Eventually, the bank successfully petitioned to lift the stay on foreclosure, foreclosed, and found that they had to invest \$700,000 back into a property which had not been maintained for four years.

How much money did the man make on this particular transaction? Well, the calculations are pretty straightforward. Assume a financing arrangement where the buyer pays less than 50% monthly rent per unit (4 years gross income per unit, purchase price). The apartment complex had 260 units. He purchased the apartment complex for a purchase price of \$3,900,000 putting down \$500,000. This left a balance of \$3,400,000.

His payments on the \$3,400,000 were \$15,800 per month. The average rental on the units (this example is not in Manhattan) was \$450.00 each. Over the period of his ownership, the slumlord kept about 85% of his units rented. So \$450.00 times 221 (85% of 260 units) comes to \$99,450.00 a month. Since the, er, gentleman, kept the property for a total of 37 months without making any mortgage payments, he collected \$3,679,650 on a \$500,000.00 investment. This means he made roughly, 19.5 % on his money every month!

That does not include the tax benefits of depreciation, nor does it include any type of overhead such as the manager he had to have on duty to make sure the rent was collected. Since the original note was a non-recourse note, the property was foreclosed, resold, and a judgment was obtained against the

partnership that owned the property. The general partner was a shell corporation, and he was the only limited partner. As a consequence, no deficiency judgment can ever be collected on this particular property.

Did the bank pursue him? No! Nor was this case referred to any legal authorities to look into.

Typically, what you see is a gentleman that will own 20-30 properties, have purchased these properties from older individuals, he will not argue the price, again, he will only argue terms. So a woman asking \$200,000.00 for a beat up 5 plex or 6-plex that most people would not touch, the gentleman will take in a heart-beat. Then begin the process of collecting rents and making no repairs whatsoever.

In the examples above, are any of these frauds in the dictionary definition? I think so. Are any of these frauds under the legal descriptions of fraud in the various states? Quite possibly, they are. What is the likelihood of prosecution on something like this - almost nil. As financial investigators, have we found this to be a wide spread practice? Absolutely!

So how do you avoid being a victim? Let's take a look at the primary victims here, the financial institutions and the people who have sold the property to a slumlord. In all instances, since you have a credit granting relationship with this individual, you may — and should — run a credit report. This will get rid of 9 out of 10 of the problem buyers. These are the people who are the professional slumlords and have unpaid bills, usually across several states. In addition you should have a property inspection prior to loan done by an engineer, a proper appraisal by Certified or Licensed Appraiser, and an environmental inspection if anything untoward is found.

The more professional slumlord — the institutional slumlord in the example above — needs to be treated more carefully. With this class of purchaser you need to have an idea of the areas in which he has operated property in the past, and under what business names. Any investigator or information broker can run a quick search and get that information. Check the superior court for the counties of concern. and for all locations where the potential buyer has operated properties. The litigation will tell you the entire tale of whether this person is a victim or a victimizer. In the above example, the attorney walked out of court and told me “Well, you got this one quicker than most, but let me tell you, usually I can forestall any litigation for an entire year. I have a death in the family, a religious holiday, 2 medical appointments, and of course a conflict of schedule. Those 5 excuses can usually get me through an entire year before I have to even appear in court.”

And remember that while we have talked about slumlords and residential property, it equally applies to the loans made to buyers of properties who are not exactly SLUMlords, but buyers of distressed shopping centers, etc. By our saying *slumlord*, we don't want you to miss the sophisticated buyer of commercial properties who "robs" lenders....

Let's just recap some of the warning flags:

- They don't argue price. This should be your number one warning flag. They don't argue price because they don't care what they are paying, because they are not going to pay you.
- They are most interested in what the monthly payment will be and how they can lower that monthly payment as much as possible, especially in the first few years.
- They wear a better suit than do you.

As we have seen in the *e-Journal* again and again, an ounce of prevention is worth a pound of cure. And again and again we are brought in, too late, by too many who get burned because they believe themselves to be too smart to need our services in exercising due diligence in financial transactions, and so never do the required — but oft-ignored — background checks, financial examinations, and physical inspections.

2. OPSEC, Economic Espionage, and Competitive Intelligence — TEMPEST

An unmarked van slows and stops. The professional inside puts down his coffee and starts in on the day's work: monitoring John Doe's computer, 10 blocks away. John is busy working on his computer with the curtains pulled against the morning sunlight. The agent watches with great interest as John reads through the cryptography and privacy newsgroups, then downloads some fiction and does his on-line banking. Everything that flashes by on John's monitor is videotaped for later review: the balance and payees of John's checking account, some decrypted e-mail that John imprudently assumed was private.

Is this scenario making you take stock of what appears on your computer screen? We all indulge in vices large and small, mentally shrugging, "Who will ever know?" In everyday life, we usually manage to keep our transgressions secret, but when it comes to information flitting across our computer screens, the answer is that there are no secrets, thanks to a relatively new, obscure form of surveillance that's a threat to your security. "TEMPEST," which stands for "Transient Electromagnetic Pulse Emanation

Surveillance Technology.” What it does is allow a simple scanning device to read the output from your monitor from up to one kilometer away. No one ever need enter your house to plant a bug or copy your floppies; it’s non-invasive and virtually undetectable. You won’t even know what hit you until all of your secrets are in the hands of your competitor.

How it works - straight forward: There is an electron gun in the back of your monitor which repeatedly fires electrons at your screen, causing different pixels to illuminate and form the text or graphics that you see. The gun sweeps rapidly up and down, sending an electromagnetic signal which constantly refreshes the information displayed on the screen. This signal doesn’t stop at the perimeter of your computer; it continues expanding outwards, seeping through the ether much like a radio wave. Exposed cables act as inadvertent antennas, transmitting the contents of your screen across your neighborhood. Information even travels back along modem lines and power cords, back into the walls and out into the world. These signals can be easily reconstructed. What’s more, a spy can differentiate between many different units operating in the same room. The signals don’t conflict or jam each other as one might suspect. Even identical units send out distinct signals because of slight differences in the manufacturing of various components. You may not think it, but your PC is hardly a self-contained unit storing information privy to you alone. In fact it is a small-scale broadcast station operating off of your desk.

A test was conducted by security professionals who built their own Tempest scanning device and took it for a test drive. We were able to view CRT screens at ATM machines, banks, a neighborhood Circle K, a doctor’s office. A bank itself was a wealth of information for anyone interested. An engineering center with open parking areas nearby with big glass windows was great, we even saw a man writing e-mail to his lover asking his lover to meet him out of town away from his wife. Titillating, but we like the industrial secrets better.

While this kind of eavesdropping has been discussed in public, most are unaware of the ease with which others can virtually read their computer screen. The individual at home really doesn’t need to worry. The corporation that has something of value needs to be very worried.

Prevention

U.S. citizens and companies can purchase snoop-proof “Tempest-certified” computers for their own use. However, the high cost of such a secure system

may be prohibitive to consumers. Even after doing this, information on how the computer was modified to meet the undisclosed emissions standards is top-secret. An affordable alternative to Tempest products, is called ZONE. "The ZONE alternative is a lighter version of the full Tempest program. The ZONE program is actually an endorsed program under NSA (the National Security Agency)." The cost of ZONE protection is significantly less than Tempest-certified units, but no definitive figures were forthcoming. "We try to price our ZONE products at what we consider commercial prices." ZONE products would be acceptable for the average commercial consumer's privacy needs, which is good news for those concerned enough with security to purchase a new computer. The bad news is that you won't have the highest level of security.

In the meantime, keep cables between components as short as possible, to reduce the length of cable that acts as an antenna. Use only shielded cable which is wrapped with metal to keep emissions within the sheath. Make sure that all computers and peripherals that they use meet the Federal Communications Commission's Class B standard, which permits only one tenth the power of spurious emissions than the Class A standard. It is also recommended that users keep the cover on their computer, mount telephone-line filter products at the jack of the modem, and to snap metallic ferrite beads over all cables so that offending electromagnetic emissions are used up in a heat sink instead of being released into the air.

Those who feel the need to protect truly valuable information can take further steps by altering the rooms in which they work. There are non woven composites, similar to wallpaper, that you can use to protect a room: The walls, the ceiling, the floors. Paste the stuff on the walls and then put paneling or regular wallpaper over it, and it pretty much makes the room secure. It blocks the electromagnetic emissions from going out. There also is translucent shielding similar to the sun tinting in an automobile that you can put on the windows.

The least expensive and easiest way to do it is electromagnetic moiré pattern masking. That's a technique using an inline box that goes between the monitor and the video card on your PC. It creates an electromagnetic moiré pattern that for all intents and purposes would keep out everybody but the absolutely most dedicated and moneyed.

What's more, the active-matrix screens now built into laptops operate without electron guns, and their emissions are much lower. When such

screens are commonly used as desktop monitors the possibility for being spied-on will be lessened.

More information could be found at the time of this writing at

<http://www.wired.com/news/print/0,1294,32097,00.html>

<http://www.newscientist.com/ns/19991106/newsstory6.html>

3. Executive Protection — Dealing with stalkers

We recently had to help a client deal with a stalker. Stalking is one of a set of ultimate forms of boundary violations, where someone becomes pathologically involved with you. Stalking becomes obvious because the behavior is obsessive and inappropriate. If you meet someone who calls you the next day, the behavior is appropriate. If you receive ten or fifteen call at work and at home, demanding your time and presence, that is inappropriate behavior. Stalking may go on for a long time. Indeed, some stalking cases have lasted more than a decade.

In general we have three goals in dealing with a stalker:

1. Keep the client from getting hurt physically and psychologically.
2. Get the stalking to end, hopefully in a timely manner.
3. Avoid hurting the stalker.

Once gaining the critical insight that one is being fixated upon, it is critical that it be made clear — without confronting, without making the stalker feel too special, and without causing embarrassment — that you are not interested in this person's attentions, and that you will not be interested in the future. It is difficult for all of us to say "No!" But it is critical that "no" be the message, because if you try to cushion your message with some excuse, your stalker is likely to consider this excuse to be merely another hurdle that must be overcome.

Once "no" has been ignored, cut off all contact with this person. This means never be in contact with them: If they write or call you once, or ten times, or a hundred times, or a thousand times, do not respond, as this merely tells them that a certain level of contact will be the price of a response. This means that, depending on the circumstances, you may need to resist the temptation of having a friend, the police, or a private detective contact the person to warn them off. And note that all of these may be involved with dealing with the problem.

Certain things may be of value in some cases: A restraining order *early on* may be a good idea if there is no history of violence and a casual relationship, while an arrest may be the best idea if there is a history of physical abuse and a long-term emotional investment. Other things, however, should always be done.

Keep written records of all contact, letters received, times you observed the person, messages left on your answering machine, crank phone calls, telephone hang-ups, and any other events which are unusual or destructive, and may be, in retrospect, part of the problem. Give copies of these records to the police and to whomever else is helping you with the situation.

Because stalking is such abnormal behavior, any intervention you take can make things better, or worse, or do nothing one way or the other. Because of this, dealing with stalkers is not straightforward, and there is no single approach that one can take. You really need the help of a professional, or a team of professionals including police, corporate security, psychologists, and private investigators, when dealing with a stalker.

Do not take this situation lightly. Laura Black, herself the survivor of a homicidal stalker, feels that you should not let the stalker drive the situation: Someone must handle it who is not intimidated. This could be the police, or someone from your employer's security or human resources department, even if the stalking doesn't occur at your workplace and doesn't involve other employees.

If you are forced to move or change your telephone number, it is definitely time to get a post office box listing for all your identification, and to tell your close friends never to give your real address to anybody without your permission.

Do not discount any information you receive: Analyze it. Take all threats seriously, and pay attention to your intuition and feelings. Notify the police when you think you can predict a violent event, even if it is only a gut feeling, and you cannot back it up with anything specific.

Stalking, though horrible and frightening, is rarely as lethal as TV and movies show, with some experts indicating homicide rates of about 2%. Other forms of violence appear more often, with estimates from 3% to 36%. The best predictor of violence is past violence.

From the corporate point of view, it is important to be as aware of this problem as of domestic violence. As with domestic violence which can spill over to the workplace, proper access control will help, and there should, of

course, be a room where an endangered employee can be hidden away until the police arrive.

In this particular case, we were *apparently* fortunate enough to be able to break the cycle and have the stalking end. The fixation had developed during a brief initial contact rather than building over time, and apparently did not have time to become ingrained in the few days before we were called in. In addition, we were able to remove all points of contact. Finally, the client was able to leave the country for a while, making here completely inaccessible. Unfortunately, only time will tell whether the stalker will reappear.

More unfortunately, stalking is one of those violent personal crimes, like assault, kidnapping, rape, and a host of others, that damages the soul of the subject. There is virtually always psychological trauma which must be understood, tolerated, and dealt with. So, even in this case, where things appear to have been taken care of swiftly and adequately, it must be assumed that there is trauma, and that care and support will be necessary for some unknown period of time. Be prepared to deal with this, and for a longer time than you might find comfortable and convenient.

For more information on personal safety, please look at *The Seven Steps to Personal Safety* co-authored by this editor. *The Seven Steps*, which has over 20,000 copies in print, is widely regarded as the leading book for civilians on dealing with violent confrontations. It can be downloaded in its entirety, and in its most current pre-fourth-printing form, free, at <http://www.lubrinco.com/lg7steps.html>

4. Technical Issues — Y2K - Next to the last

Earlier this year we discussed global positioning systems, personal computers, and mainframes.

This price of Y2K compliant equipment is increasing by the day. It will go one fire sale Jan 03, 2000 if all is well. Or it will double in price. Just look at the doubling of the cost of memory in the last two months! And they said the earthquake in Taiwan would not have an effect.

Global Positioning Systems: If they were made prior to 1988 you will need a new one.

PC's: Check the date setup, and switch it to use all four digits of the year, not just 2, Mac's are Y2K safe but will have problems with Y3K, something about which we, personally are not concerned at this moment....

Mainframes: Some of the cures for programming in the main frames have been to go back to binary code and rebuild the date function in binary code. It may work.

5. Real Stories from the Field — Peruvian guano bonds

A client recently presented several bonds along with a request for an opinion of value. He asked, “Are these bonds for real?” If so, their value could be over \$100 million dollars with accrued interest, and could be used as an asset in a corporation or sold for cash.

The bonds were 7% Gold Bonds dated May 21st 1875, without coupons, due November 1st 1880.

The bonds sold were collateralized by the proceeds of the sale of Peruvian Guano. The Bonds were guaranteed by the Peruvian Government and had the signature of the Plenipotentiary of Peru in Washington D.C. and bore the seal with the coat of arms of Peru.

This loan was agreed upon between the Guano Consignment Co. and the Government of Peru in April 1875, to rewrite a former contract between them on which Peru owed monies to the Guano Consignment Company. The government already was about to default on all of its foreign debt. In 1879 a war broke out between Peru and Chile over the rich guano and saltpeter deposits 380 miles south of Lima in the Atacama desert northeast of Antofagasta. The Chileans won and occupied Lima in early 1881. Peru, now in financial ruin, had to cede the Guano region of Tarapaca to Chile, and subsequently was torn by a civil war until 1886. Since the Chilean decree of February 22nd, 1880, guano shipments were allowed and their proceeds should have been made available to redeem outstanding foreign loans. The price of silver, Peru's most important export commodity started a long decline, which didn't help the Peruvian governments financial condition. While most of the £-Sterling notes floated in London were paid by the early 1890s, large parts of the two US Dollar loans remained in default.

The answer to the questions was almost as interesting as the history of the Peruvian Guano Bonds (Say “Peruvian Guano Bonds” out loud: It sounds wonderful and mysterious.) According to international law, countries cannot repudiate their debt because a government change has occurred. There is also no statute of limitations *per se* on debt. Thus, absent any intervening problems, these bonds were good. Unfortunately, in the 1950s, Peru offered a series of different bonds for any and all outstanding bonds upon which the Peruvian government had defaulted. The offer was good until 1975, and,

according to the World Court, settled any and all outstanding debt obligations for which the government was either directly responsible, or, as in the case of these bonds for the Guano Consignment Company, responsible as a guarantor. This is an intervening event

Another obstacle would be the fact that even without and intervening event, a collection action would need to be taken against the Peruvian Government in the World Court. As with all litigation, this would be both expensive and time consuming. The reality is that while the law may be on the side of old bond holders, practice has placed significant obstacles to its enforcement.

6. Book and Product Reviews

The Sourcebook

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

BRB Publications \$169.95 CD ROM. for \$299.00

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

This is the comprehensive Guide to State and Federal Records Sources and Educational Institutions, containing 1,320 pages, 26,000 plus records. This book is a great tool for anyone who does due diligence, background checks, litigation searches, locating people, education verification, employment verification, asset searches, business intelligence, etc. Up dates are 2 -4 times a year.

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 December 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.