

# **ÆGIS**



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

Volume 8 Number 7, July 2005

From the case files of

**The LUBRINCO Group**

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

and

**Financial Examinations and Evaluations, Inc.**

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

**Due diligence in Central or Easter Europe, or Beijing? Call us!**

**This month's features:**

- **Special Announcement**

- 1. Asset Location and Due Diligence — Yea, fraud!!!**
- 2. OPSEC, Economic Espionage, and Competitive Intelligence — We purchased what?**
- 3. Executive Protection — We are acquiring who?**
- 4. Technical Issues — Click fraud**
- 5. Real Stories from the Field — One of the smartest investment bankers we know**
- 6. Book and Product Reviews — The Criminal Records Manual**
- 7. Subscription/Unsubscription/Copyright Information**

## 1. Asset Location and Due Diligence — Yea, fraud!!!

We must admit that fraud been very very good to us. If it were not for fraud we would have no work preventing fraud: People just don't spend money preventing things that don't happen. Nor would we make any money investigating the frauds and recovering assets from the fraudsters.

But can a fraud be a good thing? Well, yes it can, if you are the buyer of a fraud-ridden company. These good frauds create opportunities to buy companies that are undervalued because of the fraud. The fraud can be used as a negotiating tool to drive down the price of the company to be acquired. The good fraud can also be one of those items that the acquirer notices but the seller does not. The buyer keeps the fraud under wraps until the purchase is completed, and then works to cure the fraud, increasing the profits of the company acquired by curing the fraud.

Sellers usually use one of the following ways to fraudulently cook the books.

- **Revenue Recognition** schemes, where revenue is recognized prematurely, or where there is fictional revenue
- **Cost and Expense Schemes**, where costs are delayed, or liabilities are not recorded
- **Over Stated Assets**, where the value of assets are too high, or the assets don't exist
- **Understated Liabilities** where the liabilities are buried or not disclosed
- **Related Party Transactions**, not done with a *bona fide* third party, that may have quantity and quality issues
- **Misappropriation of Assets**, missing assets, or failure to record the loss of assets
- **Management's Discussion of Financial Statements**, where many liabilities are omitted or glossed over

So what is a good fraud from the buyer's perspective? A good fraud (for the buyer) is any fraud that can be detected and deterred. Once detected it can be dealt with to reduce cost and increase earnings. As noted above, these frauds can be in a number of areas such as cost of materials where the seller is

paying a kickback. Or loss of inventory thought theft or misappropriation. Or the payables department sending checks out to fake suppliers or ghost employees. Or checks paid for fake returns. And, of course, when buying a small closely held business, the former owner can no longer skim revenue.

A dollar lost to fraud goes right to the bottom line. Fraud elimination is an immediate profit enhancer. Gross margin increases, profit increases, and, if you are a public company and trade at a PE ratio of 15, even a small increase in profitability by eliminating fraud in an acquisition can have a very dramatic effect on your stock price.

The flip side of this is that if the sellers have been sloppy, and have not rooted out fraud – even fraud by the owner – they end up selling their company for a value much below what the company, not riddled with fraud, would otherwise sell.

Our experience is that most companies not aware of fraud suffer a loss equivalent to about 5% of revenue, with some as high as 19% of revenue.

## **2. OPSEC, Economic Espionage, and Competitive Intelligence — We purchased what?**

It is estimated that 70% of a modern company's value lies in its intellectual assets. As discussed in detail in a recent article by one of our editors, Richard Isaacs, in *Mergers and Acquisitions Magazine*, a merger can be a very leaky time for information, with disgruntled employees offering information along with their bodies when approaching new employers, people outright selling information, or simply people just being more careless than usual.

M&A is the time for the buyer to go through the acquisition candidate's assets, both physical and intellectual, and make sure they are all still in place. Then a significant effort needs to be made to insure that the intellectual property assets have not been compromised through theft, disclosure, or sloth. The theft of intellectual property can occur from many locations and in many ways. Thus it is prudent, as part of the initial review of the company, that the Letter of Intent cover the continuing integrity of the acquisition target's intellectual property, clearly spelling out the duties and responsibilities of the target, and what they need to do to secure the property.

As part of the due diligence process, verify that there is an OPSEC program in place, as required by Sarbanes-Oxley. If no such program is in place – and it won't be – tests to see if the IP can or has leaked should be devised and used. As a last resort the acquiring company should put a portion of the

acquisition funds into a “claw back” escrow so that if theft, misrepresentation, or loss of IP has occurred, it can be dealt with through the escrowed funds, as opposed to chasing down a seller to get funds back. The “claw back” escrow is also an effective means to deal with the no-compete clauses many sellers also face.

Thus, in the purchase of a business, you need to:

- Identify the intellectual property
- Ensure it is titled correctly
- Check on the protections before and during the assessment phase
- Protect against undiscovered losses through transaction management.

### **3. Executive Protection — We are acquiring who?**

Acquisitions of companies infer the acquisition and responsibility for all of the company’s employees. And often, with responsibility, comes liability.

In many of the acquisitions with which we have assisted our clients, a big item often overlooked – because it is not there – is what information is missing from the personnel files. What is usually missing is an employee pre-hiring background report for each employee. Some employees were hired so many years ago that, quite frankly, it was not a big deal to hire someone without a background check.

So not only do you have employees with no background checks, you may have employees who have been employed for a number of years with “legacy” issues. In one company that was acquired by someone who later became our client, they were faced with multiple issues.

The acquired organization was a delivery company. Not only had the previous employer systematically underpaid their employees for the last 9 months, but, our investigation revealed, many of the employees were ex-cons and violent felons.

The acquiring company did two things: They, crosschecked time cards to pay, and they matched and checked driver’s licenses. That was it.

What they failed to check was the policy that no one was paid until they had their first call for delivery, even though they were in the yard, sometimes for hours, before they began their day. As it happens, this is against their contract, which states they have to be paid from the moment they report for work.

It was a very costly disaster when the new owners were forced to pay all of the back pay. The new CEO contested this decision very publicly, and he was threatened with physical violence, by people who had had been violent in the past, according to subsequent background checks.

This acquisition was a dual failure. It failed on economic terms that should have been discovered and avoided pre-acquisition, and it failed on safety issues for the executives, who for several months, were taken to and from work by armed guards.

#### **4. Technical Issues — Click fraud**

Advertisers generally hope a banner ad will do one of two things. Ideally, a visitor to a Web site that posts a banner ad will click on the banner and go to the advertiser's Web site. This is called a clickthrough. In this case, the banner ad has brought the advertiser a visitor they would not have had otherwise. The banner ad is a real success if the visitor not only comes to the site, but also stays and buys something. Clicks or Click-throughs are defined as the number of visitors who click on the banner ad linking to the advertiser's Web site. Publisher sites sell banner ad space on a cost-per-click (CPC) basis.

Click fraud can be initiated through an automated click generation method, or by humans. A common method is by using online robots or "bots," that are programmed to click on advertisers' text links that are displayed or listed in search queries. Another method is to employ low cost workers (another way to outsource fraud offshore) to click on text links and other Internet advertisements. A third method is executed by employees of rival companies who click on competitors' ads in the hope of exhausting the competitors' marketing budget.

Although click fraud has been happening since the cost-per-click pricing model was implemented, it has only recently received a lot of attention. This is due to, among other things, online advertisers becoming more sophisticated with respect to the cost-per-click pricing model. Another reason for the increased exposure relates to the greater competition for desirable keywords, which has resulted in a marked increase in the price paid by some advertisers for certain keywords, which in turn has resulted in a substantial increase in the overall cost of per-click programs for most advertisers.

The problem is quite serious as the cost for advertisers can be relatively high in some sectors. In mortgage refinance or legal, it could cost advertisers several dollars per click.

Interestingly, some advertisers have not pushed the issue with search networks out of a fear of jeopardizing their relationship with them. It is impossible to measure with accuracy the extent of click fraud. However, some estimates put it as high as 50 percent of total ad clicks!

Technologies that measure click rates have been developed to curb the trend of click fraud. For example, <http://www.whosclickingwho.com/> sells technology to examine click rates and sales that result from paid searches.

Another approach to fraud-detecting technology is a tracking system that analyzes Web traffic logs to detect consistent patterns of behavior over a period of time. For example, if a page is turned every 1.5 seconds over a period of time, the traffic might be flagged as suspicious.

With the ever-increasing amounts of money being spent on per-click advertising, and the great potential for abuse inherent in the system, it is no surprise that the anti-fraud click business is in its infancy, and will grow more sophisticated over time.

## **5. Real Stories from the Field —**

### **One of the smartest investment bankers we know**

That would be Fred Newcomb, Sr. – Jr. is real good, too – of Newcomb and Co. Fred gets this honor (no cash, just honor) from the way we watched him handle an investment banking investment on which we worked.

Fred was looking at a tech-based company, and thought it had merit. It was small, and had a narrow niche. The due diligence on the company, and its principals, turned up \$35,000 in unpaid bills, and two secretaries who some of the engineers had tried, unsuccessfully, to coerce into their beds.

Fred paid off the debt and the miffed secretaries, and cleaned up the company managerially. He also tightened up the ties to, and protection of, the intellectual property. He then asked us to work with the company's engineers to develop a list of all of the competitors, and rank the competitors according to quality of competing technology, as well as the quality of the engineers behind the competing technology.

Of the 14 companies we found, 11 were of interest either because they had reasonably good technology or they had good engineers. The three remaining companies had neither good engineers nor sufficient funding. These were ignored.

We then drew up a list of the “gold collar” workers (a “gold collar” being that worker who is so important to the company that if they were to leave the

company would fold) in each of the 11 companies, and a decision was made either to buy out their company, or to hire the engineers away from the competition. Four of the other companies were acquired, and the “gold collar” workers were recruited away from the remaining competitors.

Thus, when the company was finally funded, Fred had to fund the company at about twice the level initially requested, but there was no effective competition left. The small tech company developed well, is very profitable, and to this day has a virtual monopoly on the technology.

The moral of this story is that if you are smart and adequately funded, you can find problems in an acquisition and deal with them. Part of an acquisition such as this should be competitive intelligence, allowing a strategic decision was made to acquire good companies, hire the good engineers, and capture all of the narrow niche technology under one roof.

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

*The Criminal Records Manual*

Derek Hinton

Facts on Demand Press ISBN: 1-889150-43-6 448 pages \$28.95

<http://www.brbpub.com/books/details.asp?ProductID=106> 1- 800-929-3811

If you have people who do pre-employment background investigations – or even post-hiring screening – they should have this book.

Besides having information on how to access records, it has extensive information on the legal issues, with the Fair Credit Reporting Act (FCRA) with FCRA conflicts and interactions with state laws, with Title VII, and with a host of other issues that frequently trip the unwary.

This book is well-used by the staff at Financial Examinations & Evaluations, and highly recommended for those whose companies prudently have people on staff to do necessary screening.

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

•• **ÆGIS** is supported and maintained by voluntary efforts. This publication is owned, published, and copyright © 2005 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@feeinc.com).

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

- **Sarbanes-Oxley Section 404 OPSEC compliance.**
  1. American businesses lose \$300 billion annually to competitive intelligence, economic espionage, and information theft.
  2. Sarbanes-Oxley requires internal controls tracking the costs, and impact on valuation, of competitive intelligence, economic espionage, and information theft.
    - LUBRINCO provides private sector access to OPSEC, the government-standard process for identification, valuation, and protection of intellectual property and critical information from competitive intelligence, economic espionage, and information theft.
- **International asset location and due diligence.**
  - Location of concealed assets in fraud, theft, and divorce.
  - Due diligence to prevent fraud and loss in China, Central and Eastern Europe, Central Asia, the offshore financial centers, Latin America, the Caribbean.
  - Financial fraud and anti-money laundering program development and training for compliance with the US *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 **LUBRINCO** and its services, or for the archive of all past issues of **ÆGIS** in PDF format, please go to <http://www.lubrinco.com/>.

Subscription to **ÆGIS** is available for \$15 per year in North America and \$20 per year outside of North America.

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

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

If there is a topic that you would like to know more about, send it to [aegis@lubrinco.com](mailto:aegis@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**, send it as an attachment to an e-mail to [aegis@lubrinco.com](mailto:aegis@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** constitutes a license to **LUBRINCO**, 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**, you may do so freely as long as appropriate source, copyright, accreditation, and link to the **LUBRINCO** Web site is included. This should be in the form

*Article Title*, from the July 2005 **ÆGIS** (© 2005 **LUBRINCO** & FEE), to be found at <http://www.lubrinco.com/>.

**ÆGIS** 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** 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**.

Please be safe, and be smart.