



ÆGIS journal

Addressing threats that affect your bottom line

Volume 12 Number 5, May 2009

From the case files of

LUBRINCO

<http://www.lubrinco.com/>
1-212-695-1759

and

FE&E CLARITY FROM COMPLEXITY
Financial Examinations & Evaluations, Inc.

<http://www.feeinc.com/>
1-480-838-1728

Business in Bogotá or other high-threat areas? Call us!

This month's features:

- **Special Announcement:** Please see the new **LUBRINCO Web site** at <http://www.lubrinco.com/>
- 1. **Asset Location and Due Diligence — Checks**
- 2. **OPSEC, Economic Espionage, and Competitive Intelligence — RAF blackmail? Maybe...**
- 3. **Executive Protection — Be responsible**
- 4. **Technical Issues — Spyware for smartphones**
- 5. **Real Stories from the Field — An interesting check fraud**
- 6. **Book and Product Reviews — iYogi**
- 7. **Subscription/Unsubscription/Copyright Information**

1. Asset Location and Due Diligence — Checks

Processing and reconciliation is not keeping up with policies, technology, or fraudsters. We are getting some interesting comments on this from the corporate treasury world.

Current Situation

For bank accounts that utilize Payee Positive Pay, what is the use of a check security policy that currently mandates the use of 14 features? This has become an issue with our Third Party Administrators (TPAs) who use our company owned accounts to issue checks. Having so many features prohibits TPA's from using their own check stock, which only contains a handful of security features. Consequently, ordering low volume check orders (to comply with the security policy) becomes expensive... bordering on cost-prohibitive. In this day and age of Payee Positive Pay is utilizing security features even necessary? And if so, is there consensus as to which features would be considered mandatory to prevent fraud?

Comment

Most bank contracts that govern check-writing accounts now require "commercially reasonable" fraud-prevention measures. If you fail to exercise such "commercially reasonable" vigilance, then you will be held liable. Of course any time you have a loss, this is the first claim they make. Whether "commercially reasonable" is 14 or 40 features ... who can say?

So yes: Use security features. The tough part is finding that sweet spot that constitutes "commercially reasonable" without being financially (or technologically) unreasonable. This usually requires a letter ruling from your bank – and they will squeal like a stuck pig since is not something they have done before.

Current Situation

A check payable to a vendor was intercepted somewhere along the way. A duplicate check was then produced with a different payee. The original check was never presented. The reproduced check was presented and not caught in positive pay because the dollar amount and check number were valid and tied to the positive pay log. Once we realized what had happened, we attempted to return the check as altered payee, however the bank of first

deposit denied the claim stating that the check was counterfeit and not altered and we didn't respond within the time frame for counterfeit items.

This happened to another client just last week. The only way they knew was the bank's Loss Prevention department happened to review it, think it was fraudulent and called them to confirm the validity of the payee.

The duplicate check was of very good quality all the way to the correct "Pay Amount" down to the dollar amount box Thankfully, the bank called first thing on the morning of the day after it was deposited and the client's bank was able to immediately return it as fraudulent. The client also put a stop payment on the original check and took it from their positive pay file. The check amount was more than USD\$23,000.

Solution

The incremental costs of adding payee validation is well worth the investment when checks of that amount are being issued. Further, this scenario suggests that to effectively combat this we change the following:

- 1) Printing of checks remained as a function within Accounts Payable, with two designated individuals, along with one alternate as being an authorized employee for this, and that all three undergoing annual due diligence reviews, which include both background checks and evaluation of the employees' credit report information.
- 2) Check distribution (stuffing, mailing and special pick up) was moved to another group, under video surveillance. Most loss was associated with these processes.
- 3) Consider use of ACH as the preferred payment method, especially for any items of higher value (e.g. anything over USD\$10,000).
- 4 All payments over a certain threshold (e.g. USD\$20,000) must be electronic, ACH, wire etc...

Another Current Situation

Several micro ACH payments have been hitting our deposit account. While losses associated with any one transaction is not large, losses can quickly begin to add up.

Solution

Set up a deposit account that is just a deposit account. No payments to other accounts other than a daily or week sweep to a COH (Cash On Hand) account. When it is time to pay bills, transfer only that amount necessary to

pay your bills to the disbursement account. Use all of the positive pay features and move all of the employees and vendors to electronic payments. This is a good carrot since, if paid by electronic payment, they can get their payments even earlier and no hold on funds when deposited.

It takes a bit of time to get it set up, but it is so worthwhile. This saves approximately \$9.50 for every check issued and mailed.

Reality

Most of the policies in effect at both the bank and at the corporate client firm are years old and probably have not been updated to fully address new payment options, changes in the patterns of frauds, and solutions to both combat fraud and reduce the cost of making and taking payments.

A thorough review of policies and processes needs to be undertaken with the Accounts Payable (A/P) and Accounts Receivable (A/R) departments to bring them up to speed with what your banks can do. Revise policies accordingly.

After you have appropriately revised you policies and procedures, please, please inform your insurance carrier. It is highly likely that when your fraud and theft insurance policy was issued, you were rated based on a policy put into effect several years ago. Now that you have updated the A/P and A/R practices, to increase speed and reduce fraud, request a re-rating or re-evaluation by your insurance carrier.. Even if you do not get the lower rating, understand that it is in your best interest to provide updates to the policy and procedures manual that you initially submitted to the insurance company at the time of underwriting. Otherwise, this might be used as a potential excuse for your carrier to deny a claim, under the guise that the changes were never submitted for approval (something your policy doubtless states in the little teeny type).

2. OPSEC, Economic Espionage, and Competitive Intelligence — RAF blackmail? Maybe...

According to an article in the Guardian, (<http://www.guardian.co.uk/uk/2009/may/24/raf-military-files-stolen-blackmail>), three hard drives went missing from RAF Innsworth, Gloucestershire, last September. Originally this was thought of as a sort of “ho-hum” event, as it was believed that only the bank details and home addresses of 50,000 servicemen and women were on the computers.

However, it now turns out that the missing computer drives also contained information on 500 senior RAF staff, with access to Top Secret information,

including details of criminal convictions, investigations, precise details of debt, medical conditions, drug abuse, use of prostitutes, and extra-marital affairs including the names of third parties. This has been the cause of some alarm, as these people *might* then be open to blackmail for secrets.

Security is always a balance of risk versus cost. In this case, let us assume that the RAF thought there was some risk attached to having this data on hand, and had to balance the risk of it being stolen and used against the cost of protecting it. Let's say that they decided it was worth encrypting the data, and looked around for off-the-shelf software. How much would it have cost to protect the three hard drives?

We use Private Disk from RIT Labs (<http://www.ritlabs.com/en/products/pd/>), who make the e-mail programs we use (The Bat! and The Bat! Voyager). Assuming that the RAF bought three copies retail at \$29 each (we paid \$19 as users of The Bat!), it would have cost them \$87, or £53.08. But I'm betting that even if it cost them five times (or fifty or one thousand times) that to secure the computers, they would have been wise to pay the price.

The real question, of course, is not whether the RAF – and every other government agency in the world – is silly not to encrypt their data. The real question is whether or not *your* data is encrypted. If your computer – such as your personal or your company issued laptop – disappeared would there be information on it that you would not want floating around? We believe the answer would be a resounding “Yes!” Are there any company desktop computers that have unencrypted data on their hard drives? We suspect there are.

You'll find a wide variety of commercial encryption packages floating around. Using them is trivial, and generally only involves clicking on an icon and entering a pass-phrase. The cost is low, and the security is high.

3. Executive Protection — Be responsible

One of our favorite television shows is *Clifford the Big Red Dog*. In one episode (THE KIBBLE CROOK, 126a), T-Bone can't resist sneaking a bite – well, okay the whole bowl – of Cleo's new dog food. When Cleo gets upset, T-Bone blames it on another dog and sends our fearless friends on a wild goose chase. But T-Bone ultimately confesses that there is no other dog, and he learns that he must take responsibility for his own mistakes. *Clifford's Big Idea: Be Truthful*.

This is good idea not only for children, but for grown-ups as well. Doing bad things has the potential for getting you in trouble, often with significant and potentially grave consequences. Unfortunately, covering up the bad things only

makes the situation worse. We have certainly seen cases of embezzlement or other forms of fraud that escalated to homicide. While the consequences of embezzlement are bad, the consequences of homicide are worse.

It would certainly be a lovely world if nobody did bad things. And, in fact, we would be delighted to be put out of business because people stopped doing bad things. Failing that, we would like to see people try to reduce the consequences of their actions by cutting short their escalation of crime.

4. Technical Issues — Spyware for smartphones

This morning a call came in from an associate. The voice quality was bad, so we said “You got a new smartphone! Blackberry or iPhone? As it happened, it was an iPhone.

Smartphones are handheld special-purpose computers that connect to the internet using one or another of the wireless broadband protocols. The phone part generally gives the impression of having been thrown in as an afterthought, so that many people carry a Blackberry for e-mail and a mobile phone for making calls, or an iPhone for the really cool things it does and a mobile phone for making calls. Those indifferent to voice quality, however, or those not wishing to carry two devices will often just use the smartphone to actually make calls.

The problem with this is not so much the voice quality – that is merely an annoyance for the person speaking with them – but the fact that these little computers using the Windows or Symbian OS (and, according to the ads, BlackBerry) are apparently very easily hacked. We do not know any smartphone user who has bothered to install anti-malware software, which is surprising considering that there sure is a lot of software designed to allow you to hack smartphones. You can look at <http://utilities.flexispy.com/checkphones.jsp?p=0> to see one vendor’s list of phones they can compromise.

So, what can the spy do? Worst case listen in to every call you make, real-time, and get copies of your text and e-mail messages, as well as activate the phone to hear what is being said near it. For the iPhone, the worst that can be done *that we have found* is to get copies of all SMS, e-mail, GPS locations, and the logs of all phone calls made. We suspect that real-time listening to conversations are available now, or will be available soon.

The good news is that in order to hack your phone the hacker needs physical access to it. Installation of the malware is often done via Bluetooth, which means that the hacker has to link your device with his to make the transfer.

The easiest way to prevent this is to make sure that nobody else ever has access to your smartphone. This issue of access is significant

Thus, as an example, if you were using two smartphones with encrypting software installed, you could make secure encrypted calls. But if you let them be out of your control for as little as under three minutes and the phones could be compromised, and the encryption meaningless – at least to the spy.

There are also clues as to your being tapped. In some cases your battery could be running down quicker than it should, because of all the extra transmission. In some cases the batteries will be warm, as often happens during long calls. You may notice increased GPRS or SMS activity on your bill. Your phone might light up at odd times, when you are not doing anything with it. And it might make nearby loudspeakers buzz at randomly appearing times, much the way they would if you were actually making a call.

5. Real Stories from the Field — An interesting check fraud

A woman had her purse stolen, and notified all the appropriate people.

Sometime thereafter another woman went into a branch of the bank and made a bad-check deposit of \$5,000 into the compromised account. She said she needed her account number, which she was given (she had the stolen ID), and asked for the balance, which was a bit over \$3,900.

She then went to another branch and made another bad deposit of \$5,000 and asked if she could get \$3,900 back in cash, which she was given, since there was an available balance of \$3,900.

While there were systems in place to prevent this – there was a flag on the account – they didn't work. This is likely a problem that will continue for some time.

This is a simple fraud and very successful. The question for us, the folks who try to prevent frauds, is what could be done to stop the frauds yet not interfere with the business process? Even something as simple as a note on the account that this account may be compromised or simply ignored, as happened in this case. Asking for two forms of photo ID *should* work, but in this case the faux customer had all of the real customer's ID, and looked enough like her to pass.

6. Book and Product Reviews

iYogi

\$139.99/year

<http://www.iyogi.net/> 1-800-237-3901

The difference between the computer amateur and the computer professional is that when something goes wrong the amateur tries to fix it and the professional calls the help line. If you are at work, and work for a large enough company, you can call the support desk. But what do you do at home?

At the end of last year we came back from a four month absence, and discovered that while we were away one of our guests had made our computer non-functional, apparently by simply pushing the off button on the computer (which also served as a mail server, and was normally never turned off) each night after he had finished doing whatever he did online.

I somehow ended up calling iYogi, which one of the other people staying at our place thought was Microsoft. In fact, iYogi has over 500 Microsoft Certified Technicians, is staffed 24 hours a day, and offers Dell, HP, and Microsoft support. The technician took over my computer, and managed to deal with the missing internal registration (whatever that is) that was preventing the machine from booting.

If you have a technical problem with your computer, and don't know where to turn to solve the problem, iYogi is a great resource!

7. Subscription/Unsubscription/Copyright Information

•• **ÆGIS** is supported and maintained by voluntary efforts. This publication is owned, published, and copyright © 2009 by The **LUBRINCO** Group Ltd, Inc. and Financial Examinations and Evaluations, Inc. It is edited jointly by Richard Isaacs (RBIsaacs@lubrinco.com), L. Burke Files (LBFiles@feeinc.com), and Terry Phillips (TPhillips@aegisjournal.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.

- **International asset location and due diligence.**
 - Anti-money laundering, financial fraud, and anti-corruption program development and training.
 - Statutorily mandated AML independent examinations and program reviews for financial institutions and gatekeepers.

- Investigation and location of missing or concealed assets, related to fraud, theft, and divorce.
- Due Diligence to prevent fraud and loss, as well as validate potential business partners or potential business acquisition or merger. LUBRINCO has significant expertise in performing Due Diligence in China, Central and Eastern Europe, Central Asia, the offshore financial centers, Latin America, and the Caribbean.
- **Identification, valuation, and protection of intellectual assets and critical information.**
 - American businesses lose \$300 billion in revenues annually to competitive intelligence, economic espionage, inappropriate disclosure, and information theft.
 - **LUBRINCO** provides private sector consulting access to OPSEC, the government-standard process for identification, valuation, and protection of intellectual property and critical information.
 - Implementing an OPSEC program is likely to increase revenues for an at-risk operating group by \$75 million.
- **Protection of executive 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.aegisjournal.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, send an email to subscribe@aegisjournal.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, send an e-mail to unsubscribe@aegisjournal.com.

If you know of anyone else who should be receiving **ÆGIS**, please send their e-mail address to subscribe@aegisjournal.com.

If there is a topic that you would like to know more about, please send your request to editor@aegisjournal.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**, please send it as an attachment to an e-mail to editor@aegisjournal.com.

Submission of an article for publishing consideration 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 **ÆGIS** Web site is included. This should be in the form

Article Title, from the April 2009 **ÆGIS** (© 2009 **LUBRINCO** and FE&E), to be found at <http://www.aegisjournal.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.