



PROXIMAL CONSULTING

One The Parade Mews Marlborough Wiltshire SN8 1NE
Place du Bourg-de-Four 25 1204 Genève Switzerland

Tel: +44 (0) 1672 516725

Fax: +44 (0) 1672 516759

E-mail: info@proximalconsulting.com

www.proximalconsulting.com

THE MONEY LAUNDERING & BUSINESS CRIME MITIGATION FIRM

due diligence *training *asset tracing *compliance & assurance *investigations *strategic advice
*research

MONEY LAUNDERING & BUSINESS CRIME NEWSLETTER ISSUE 14 – SEPTEMBER 2002

This newsletter is published regularly and delivered to clients and contacts of Proximal Consulting by e-mail

CONTENTS

- Money laundering through credit cards
- The old ones are always the best – a warning on “High Yield Investment” frauds
- Global News roundup
- A blatant piece of self promotion!
- Due Diligence & Fraud Prevention Warning List
- The Final Word

MONEY LAUNDERING THROUGH CREDIT CARDS

The United States General Accounting Office report on money laundering using credit cards (published in August 2002) rather removes the need to read the full 56 pages of the document by subtitling it “Extent of Money Laundering through Credit Cards is Unknown”. That having been said the report makes some interesting observations – and highlights the fact that the use of credit cards for laundering may be yet another compliance weak spot:

- There is a perception that credit cards are not used in the placement stage of money laundering but might be used in the layering or integration stages
- Most law enforcement officials interviewed were unable to cite any specific cases of credit card facilitated money laundering in US financial institutions
- There are very few money laundering Suspicious Activity Reports filed in respect of credit card usage
- However there is evidence that “credit card accounts accessed through banks in certain offshore financial secrecy jurisdictions could be vulnerable to money laundering”

- Credit card industry representatives said that they did not have AML policies and programs focused on credit cards because they considered money laundering using credit cards to be unlikely. Whilst the credit card industry believes fraud prevention methods used in credit card applications and processing will help identify launderers and laundering the US Treasury believe that these systems are “a starting point for appropriate anti-money laundering safeguards, but alone they are not sufficient”
- The average value of a US credit card transaction is \$70, whilst Fedwire and Clearinghouse Interbank Payment electronic payments averages are \$3.5 million and \$4.9 million respectively. Thus the argument is that credit card transactions pose far smaller risks
- Examples of how credit cards could be used in the laundering process include: the launderer prepays his credit card using funds already in the banking system, creating a credit balance in the account. He then requests a refund, presumably in the form of a cheque which further obscures the origins of the funds; the launderer uses illicit funds already in the banking system to pay his credit card bill (thus integrating the funds)
- The report highlights the risks of the use of credit cards associated with banks in offshore jurisdictions to launder money but comments that the extent of this activity is unknown

Our own take on this is that one of the advantages offered to launderers by credit cards is that such pieces of plastic are a global currency. Thus if you can obtain a card in a jurisdiction (or a particular financial institution) which has non-effective fraud prevention and AML systems than you can use your card anywhere in the world and on the Internet. Thus the launderer can purchase anything anywhere (and withdraw cash) then pay off the monthly bill without generating any red flags. This type of usage would be particularly attractive for example, to a terrorist or an individual planning a terrorist attack. Information concerning the 9/11 terrorists suggest that they made numerous transactions and cash withdrawals with debit cards, which are not a million miles away from credit cards. Certainly, solely the use of credit cards would not facilitate a successful money laundering operation: but as one part of a complex and well thought out methodology, credit cards could be a valuable tool.

THE OLD ONES ARE ALWAYS THE BEST

The story of Graham Hammond allows us not only to retell an age-old tale but also to warn against “high yield investment” frauds that are once again on the increase.

On 16 August in Norwich (UK) Graham Hammond was sentenced to five and three years consecutive imprisonment after pleading guilty to twenty counts of false accounting. In a classic Ponzi scheme that lasted six years Hammond obtained £1.34 million from his investors. This scam began in 1994 to cover currency trading losses he had made whilst working as an independent financial adviser in Norwich. To repay his clients he lured new investors into a fictional fund that promised returns of 20 per cent.

In classic style, Hammond used this new money to repay his old customers. But then the new investors cashed in their positions – so Hammond set up a new fictional fund and took money off new clients to pay back previous ones.

Hammond’s company FCS Fund Management Limited ended up with offices in Norwich, Dubai and Hong Kong. Salesmen operated in the UK, Europe and Middle East – particularly targeting expatriates. In the end the shortfall between what Hammond was supposed to be holding for clients and what actually existed was £10 million. On the way Hammond stayed at luxury hotels, was a regular at casinos and opened a club in Bangkok called “Out of Bounds” Hammond claimed that he was the victim of a fraud by “seemingly rich and reputable Swiss brokers”. This and other such comments led the judge to observe that “I also note that you see yourself as a victim of the dishonesty of others. It is a measure of your self-deception that you do not chose to see yourself as you are.”

Across the Atlantic on the day before Hammond's sentencing another verdict was delivered in a strangely similar case. John Wayne Zidar was found guilty of fraud and money laundering charges involving cheating 2,500 people out of \$74 million. Zidar, a 59 year old former Washington state resident operated another Ponzi Scheme with Steven Moreland, who was found guilty of 14 charges. They promised investors – many of whom were anti-government “patriots” who believe that the US economy is inherently unstable – returns of 120%. And how was this return to be achieved? Through access to a semi-secret entity of wealthy business interests called the “private economic arena”. Presumably Zidar had gained access to this closed society when he was working as a night janitor at a chain steakhouse in Florida in 1997. Because just after that he set up Vista International, Oakleaf international and Rosewood International investment clubs – all of which promised investors large profits with little (or no) risk. Zidar also claimed that he had access to one of the half dozen traders worldwide who controlled “prime bank instruments” which are quietly issued by the world's largest banks and accessible only to a few select individuals.

Investors who purchased one “unit” of shares for \$1,294 in one of these clubs were promised a \$3.4 million return in 10 years. And surprise, surprise: old investors were paid with the money from new investors. Until of course, with the awful logic of predictability, the new investors dried up. On the way Zidar and Moreland bought houses, expensive cars and laundered millions of dollars through bank accounts in Samoa, the Bahamas and Costa Rica.

“High yield investments” or “high-yield programs” offering unattainable returns have always been with us – and probably always will be. However this particular fraud type seems to be currently on the increase. The guidelines contained in our White Paper 3 (on Advance Fee and Financial Instrument fraud) are equally relevant to this type of scam. This white paper, together with numerous others, can be found on our website: www.proximalconsulting.com

GLOBAL NEWS ROUNDUP

WORLDWIDE: The number of reports of maritime piracy rose to record levels in the first quarter of this year. Increasingly such attacks are also extremely violent: in November 2001, 23 members of a Hong Kong freighter were murdered and thrown overboard in an attack. It is now believed that many attacks are by sophisticated organised crime groups who take vessels by force and turn them into re-named and re-registered “phantom ships”. Somalia and Indonesia are considered to be piracy hotspots, with the Straits of Malacca - between Indonesia, Malaysia and Singapore – being the most dangerous location in the world with a third of all attacks occurring there.

NICARAGUA: During August Arnoldo Aleman (known as “Gordoman” – Fatman) the former president of Nicaragua (he held office until January this year) was charged with stealing \$100m of state funds during his stay in office. He is currently the leader of the country's congress and thus immune to prosecution. Mr. Aleman, his sister, brother, daughter, three former ministers and seven others have been charged with money laundering, fraud and misuse of state funds. The US Ambassador to Nicaragua confirmed that a US investigation was also underway and that “this is one of the biggest frauds committed in any country”. 48% of the country's population lives on less than a dollar a day: whilst Aleman is accused of (amongst other things) using his state backed credit cards to pay for two nights at the Cabaret Lido in Paris (\$10,000), buy Egyptian carpets (\$22,530) and spending thousands more on jewels, hotel stays and bar bills.

UNITED KINGDOM: Another story in the series of “the old ones are always the best”....Fraudsters in the UK obtained dozens of false passports using the same scam as the assassin in Frederick Forsythe's “The Day of Jackal”. The three men made over £600,000 in one year from stealing the identities of dead babies, then getting duplicate birth certificates and using them to obtain passports which they sold for £30,000 each via adverts in the “international Herald Tribune”.

SOUTH AFRICA: In August 15 Nigerians were arrested after luring people to send them money by pretending to be from the South African Central Bank. The gang operated by e-mail and promised to pay its victims a commission for looking after \$10m. The victims were directed to a website that

looked similar to that of the South African Central Bank. The fraudulent website requested that its visitors made an advance payment to cover insurance and other costs. The gang also diverted phone calls and used fictitious e-mail addresses. The truth only dawned when the promised large amounts never materialised!

SPAIN: At the end of July Mario Conde, described by "El Pais" as "once the epitome of business success and glamour in Spain" returned to prison to serve 20 years for fraud and embezzlement committed during the time he was chairman of Banesto Bank. The Spanish Supreme Court also jailed a further five members of the former board of Banesto: all were found guilty of generating a "black hole" at the bank totalling € 3.4 billion. In the period of 1987 to 1993 funds of the bank were regularly diverted into offshore accounts and phantom companies. Conde and his associates subsequently embezzled these funds. The long running investigation and trial resulting in Conde receiving a 10 year and 2 months sentence in March 2000. With supreme irony, Conde appealed that sentence – but in July the Supreme Court issued a 434 page ruling, and increased Conde's sentence to 20 years!

A BLATANT PIECE OF SELF PROMOTION

Well at least we're honest about it! Peter Lilley's new book "Hacked, Attacked & Abused: Digital crime exposed" is published on 19 September. Covering all aspects of electronic crime the book is described by the author in the following terms:

'This book does not seek to present an alarmist vision of the Digital Age. But neither does it attempt to airbrush out the grave risks and dangers that are ever present in this brave new environment. This is not a technical book, in that it does not reproduce lines of software code that will magically solve all of our digital security problems. What this book does attempt to do is describe and analyse the risks inherent in the sustained and continued reliance on technology. Primarily this is viewed from a business focus, but as ultimately we are all customers, the perspective cannot be a narrow one.'

Further details of "Hacked, Attacked & Abused" can be found on our website, www.proximalconsulting.com together with an on-line ordering facility.

DUE DILIGENCE & FRAUD PREVENTION WARNING LIST

We detail below various dubious, questionable or fraudulent entities and transactions that we have recently become aware of. As always – Caveat Emptor (Buyer Beware)!

1 CENTRAL BANK OF KUWAIT

An ongoing warning is in existence from the Central Bank of Kuwait (CBK) regarding possible fraudulent transactions involving persons claiming to be employees or representatives of the bank. CBK advise that any individual, financial transaction or instrument claiming to be related to the Bank should be verified with them first. Relevant contact points are:

Banking Operations Department – Central Bank of Kuwait

Telephone: +965 244 3425

Telephone: +965 243 6658

Fax: +965 240 3652

E-mail: bod@cbk.gov.kw

2 TRINITY SAVINGS BANK / GOLDMAN & STEIN

The Central Bank of Belize has issued a warning that these entities are not licensed to provide banking and/or financial business in Belize. Thus any proposed transactions should be "viewed with extreme caution". Goldman & Stein are operating from the following co-ordinates:

1934 Driftwood Bay
Belize City
Belize
Central America

PO Box 2235
Belize City
Belize

www.goldmanstein.com

3 WITHERSPOON, SEYMOUR & ROBINSON INCORPORATED (WSR)

The Office of the Registrar of International & Foreign Companies in Samoa has issued a warning against this company, which has been advertising on the Internet. WSR has been offering for sale capital management companies registered in Samoa and "pre approved" banking licences in Samoa and other Pacific Island jurisdictions.

WSR is not a licensed trustee company in Samoa and has no authority to sell Samoan companies and/or banks. There is no such thing as "pre approved banking licenses". The contact details for Witherspoon, Seymour & Robinson Incorporated are:

Internet: www.wsr.biz (we have also located the same website at www.wsr.cc)
Telephone: +1 646 205 8170
Fax: +1 646 365 3400

Addresses

1461A First Avenue
Suite 360
New York
NY 10021-2209

3105 North Ashland Avenue
Chicago
IL 60657-3013

9663 Santa Monica Blvd
Beverly Hills
CA 90210-4303

4 JOHN RUFFO

The US Marshals Service has issued a further warning about this person who was convicted in 1998 for his role in defrauding several banks of over \$350 million and is thought to be now attempting further fraudulent schemes. He uses both his real name and aliases.

The original fraud was highly publicised as Ruffo was posing as an official of the Philip Morris Company and arranging fraudulent leasing deals. Peter Lilley has previously written about Ruffo:

Philip Morris envisioned a project that was so secretive not even the venture's own employees would know who they were working for. Or so Signet Bank in the US were told. The tobacco company, desperately seeking cigarette alternatives, wanted to set up five research centres throughout the world explained Edward J Reiners, Chief Operations Officer of Worldwide Regional Exports, which was identified as a wholly owned unit of Philip Morris. The secret venture codenamed Project Star would need an initial loan of \$61 million to lease computers and other equipment. Signet took the bait and got other banks to participate in

the loan. The problem was that Philip Morris had no Project Star and Mr Reiners no longer worked for the tobacco giant. But none of the banks involved checked any of this. Reiners and an accomplice John Ruffo raised loans totalling \$353 million - and then started to live the highlife. Rather like a snowball rolling down a hill, the scheme gained credibility as it went along as the more financial institutions that were taken in the more genuine it appeared. Reiners and Ruffo invested in the stockmarket, expecting to pay back the loans they had received and retire on the profits. It all went wrong and the FBI arrested Reiners and Ruffo: \$13 million dollars is still missing. Reiners was given a 16 year jail sentence; Ruffo one year more. The final twist in the tale? Ruffo on his way to jail managed to simply walk away and hasn't been seen since!

A US Marshals press release and photograph of Ruffo can be found at:

<http://www.usdoj.gov/marshals/news/ruffo15.html>

5 MARYLAND INVESTMENT CLUB

The Canada Deposit Insurance Corporation (CDIC) has issued a warning concerning the activities of Maryland Investment Club which is offering fraudulent "digital investment certificates". These documents contain a forged signature of CDIC's General Counsel, Gillian Strong. We warned against this entity in our last newsletter (Issue 13, July 2002) in the following terms:

MARYLAND INVESTMENT(S) CLUB – This entity has been falsely claiming to be linked with MD Private Trust Company, a legitimate and authorised Canadian deposit taking institution. This entity operates at least two websites:

www.eprivacysecured.com/invest
www30.brinkster.com/marylandic/index.htm

which offer "high-yield international tax-free investing with as little as \$500!". We can't find a physical address on either of these websites – but one of the e-mail contact points given is on a Latvian ISP! The apparent address of Maryland Investment Club is:

33 Prince Arthur Avenue
Toronto ON

6 SUNLIFE FINANCIAL TRUST INCORPORATED

The Office of the Superintendent of Financial Institutions Canada (OSFI) has issued a warning about the activities of this fictional entity which is not an authorised Canadian financial institution. It is suspected of being part of a Nigerian 419-advance fee fraud. It is not connected with a legitimate federal trust company, Sun Life Financial Trust Inc. The details of the false entity are:

Sunlife Financial Trust Incorporated
7 Nickel Street
Toronto ON
M2H 2H9

7 ALLIED CHARTERED BANK, EQUITY SHARES FINANCIAL SERVICES & SCHWEIZER INVEST BANK AG OF SCHWEIZ

The Office of the Superintendent of Financial Institutions Canada (OSFI) has issued a warning about these three entities which are also not authorised financial institutions and are suspected of being part of various Nigerian 419 advance fee frauds. The available details are:

Allied Chartered Bank

Toronto
Ontario
Related entity: Equity Shares Financial Services

Schweizer Invest Bank AG of Schweiz
Schweizer Bank Plaza
200 Bay Street
Toronto
Ontario

8 MR. SERGIO PEGHINI & MS. PATRIZIA FUSCO

The Italian Securities Regulator (CONSOB) have warned that neither of these individuals are registered financial salespeople in Italy.

9 CAMBRIDGE INTERNATIONAL S.r.l.

The Belgian Banking & Finance Commission have warned against the activities of this company, which may be approaching members of the Belgian public proposing investments in financial instruments. The company does not have the relevant authorisation to provide such services in Belgium. The company is located at:

Via Parini 9
Milan

10 INTERNATIONAL INVESTMENTS BANKERS (aka INVESBANKERS)

The Belgian Banking & Finance Commission have warned against the activities of this company, which presents itself as a Belgian credit institution. Invesbankers has not been granted an authorisation to act as a credit institution in Belgium, neither is it authorised to offer banking services in or from Belgium or use the term bank. Additionally this entity has no effective office in Belgium. Contact details given by this entity are:

Suite #5
Rond-pont R Schuman 6
1040 Brussels

11 MORGAN YOUNG

The Belgian Banking & Finance Commission have warned against the activities of this company. It is contacting potential investors in Belgium and proposing that they buy shares in Global Food Technologies, a company which it is claimed will soon be listed on the US Nasdaq. Morgan Young does not have the required authorisations to do this in Belgium. As the Commission observes Morgan Young "uses a name which closely resembles the name of well known financial intermediaries, which may mislead the investors about its true identity" Morgan young quote the following addresses:

Avenue Louis Casa 18
CH 1209 Geneva

4/F East Tower
Otemachi First Square
1-5-1 Otemachi
Chiyoda-ku
Tokyo
100-0004

12 AMERICREST BANK & TRUST

The US Federal Deposit Insurance Corporation (FDIC) has warned against fictitious official cheques and certified checks in circulation from this non-existent US bank. This false entity gives the following details:

Americrest Bank & Trust

Post Office Box 23202
Van Nuys
California

PO Box 2012
Van Nuys
CA 91411

13 AUDI BANK NA

The US Federal Deposit Insurance Corporation (FDIC) has also warned against fictitious cheques issued by this fictitious entity. The details given are:

Audi Bank N.A.
19 East 54th Street
New York
NY 10022

Routing number: 021200957 (belongs to an unconnected legitimate bank)

Audi Bank N.A. does not exist, but a legitimate and unconnected bank, Bank Audi (USA) does exist at this address.

14 MORGAN PARIS

The Central Bank of Ireland has issued a second warning about this company, based in Spain. That gives us a timely reminder to highlight this entity and related ones (we originally referred to them in Newsletter 10 in January 2002). The main reason why we are doing this is because investors who have paid over large amounts and have so far seen nothing in return are continually contacting us. This company (and connected parties) are the subject of a fierce debate on various Internet discussion boards as to whether this is a fraud. The details that we are aware of are as follows:

- Morgan Paris appears to have taken over from where Goodman Hart & Associates left off: Various warnings have been issued about Goodman Hart. Both entities have been offering for sale shares in AdRentaCar (which in turn was the subject of a Belgian official warning in December 2001)
- Previously shares were offered for sale in Spantel Communications Inc.
- Morgan Paris operates from www.morganparis.com, which does not give a contact address. As far as we are aware this entity operates from the same address in Spain as that given for Goodman Hart
- Latest unconfirmed information suggests that two further "companies" may be associated: Raymond Lloyds and Pierce Watters (at www.raymondlloyds.com & www.piercewatters.com respectively). Neither of these websites give a contact address and both recommend stock in European Diversified Holding Co. Inc.
- Known contact details are:

Goodman Hart Associates
Ramon Gomez de la Serna 5
Edif Marbella Azul Bajo 8

Marbella
Spain
www.goodmanhart.com (now somewhat unreassuringly a blank page!)

AdRentaCar
Poligno Industrial Villarosa
Calle Carril Guetara 75
Malaga
Spain
www.adrentacar.com

15 VARIOUS WARNINGS FROM THE CENTRAL BANK OF IRELAND

In August The Central Bank of Ireland has issued warnings about the following entities:

- FRANKLIN MANAGEMENT, Switzerland
- COGAN DAVIS INTERNATIONAL, Cayman Islands
- CURRENCY ASSOCIATES, USA

16 ARROW INTERNATIONAL MANAGEMENT SERVICES LIMITED & NORMAN EDWIN STEELE

The Jersey Financial Services Commission and the South African Financial Services Board have both issued warnings about this company and individual.

The Jersey Financial Services Commission have confirmed that Arrow International Management Services Limited was a private Jersey company until it was struck off on 13 October 2000. It had not received authorisation to conduct investment business. It was located at:

Sir Walter Raleigh House
48/50 Esplanade
St Helier
Jersey

Norman Edwin Steele purported to be managing director of this company, which not only was unauthorised but also was refused a licence when it applied for one.

The South African Financial Services Board has warned against doing business with Arrow International Management Services which is now operating from:

11 Holden Avenue
Morningside
Durban

This entity is operated by Norman Steele and is not registered to conduct investment business in South Africa.

17 DREAM BOND

The Financial Services Board (FSB) of South Africa has warned against Dream Bond, a financial product that has been advertised in the country. It offers rates of return of 18.5% per year, payable monthly in advance: the advertisement states that top returns is the least the company can do for its clients (!?)

Dream Bond is not registered with the SA Financial Services Board and Danie Muller (who is behind Dream Bond) has been informed that what he is doing is illegal. The operation appears to be operating from a cell phone, as opposed to a physical address.

18 NIGERIAN / WEST AFRICAN 419 FRAUD

We are almost slightly embarrassed to once again warn against this fraud type. However judging by the number of 419 letters we receive and the feedback we get, this fraud type is alive, well and thriving. It is reported that in the US the number of reported incidents have risen by 900% between 2000 and 2001. Thus once again we advise:

- If you receive a letter or e-mail from Nigeria, Ghana, South Africa or in fact anywhere, that promises you a percentage of a large amount of money, IGNORE IT
- Under no circumstances whatsoever should you provide your bank account details, any personal or business information and you should never send any money
- Always consider the following dictum: if anything sounds too good to be true, that's because it is!!

THE FINAL WORD

"Rufus is a pimp for three girls. If the price is \$65 per trick, how many tricks per day must each girl turn to support Rufus's \$800 a day crack habit?"

- Question in a Canadian maths exam quoted in "Scotland on Sunday"

A final thought (some may say heresy) offered by George Trefgarne in the UK "Daily Telegraph": after Enron, Worldcom et al wouldn't it be better if the Mafia ran corporate life? They may be criminals, but at least they stick to their standards: following strict codes of honour, family and loyalty. This seems a refreshing change from some of the current operators in the "legitimate" business world.

IF YOU OR YOUR COLLEAGUES WOULD LIKE TO BE ADDED TO OUR DISTRIBUTION LIST PLEASE E-MAIL US AT info@proximalconsulting.com or go to our web site and use our newsletter subscription form.

IF YOU WOULD LIKE COPIES OF OUR PREVIOUS NEWSLETTERS YOU CAN NOW DOWNLOAD THEM FROM OUR WEBSITE

IF YOU WOULD LIKE TO DISCUSS A SPECIFIC PROBLEM OR PROJECT WITH US PLEASE CALL US ON +44 1672 516725, OR FAX US ON +44 1672 516759.

© PROXIMAL CONSULTING MMII

This research was prepared by Proximal Consulting and is for information purposes only.

This publication is not a substitute for specific professional advice

Any dissemination, distribution or copying of this communication without prior approval from Proximal Consulting is prohibited