



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 15 OCTOBER 2002

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

CONTENTS

- Identity Theft
- FATF Blacklist changes
- Global News Roundup
- Due Diligence & Fraud Prevention Warning List
- The Final Word

IDENTITY THEFT

Identity Theft is described by the FBI as the fastest growing white collar crime area. It is one that has a variety of uses for a criminal – it is also now becoming clear that this fraud type is also being used by terrorists to finance their operations. The FBI have highlighted the fact that terrorists use stolen credit cards, passports and Social Security Numbers to conceal their true identities and pay for their operations. In July of this year Denis Lormel, the chief of the FBI's financial crimes unit told a US Senate subcommittee that "Identity theft is a key catalyst fuelling many of the terrorists methods". He then quoted the example of an al-Queda cell that was broken up in Madrid that used stolen credit cards in sales frauds and for small purchases that did not require other identification. The group also used fake passports to open bank accounts, which were then used to send money to and from countries such as Pakistan and Afghanistan.

In an extract from his recently published book "Hacked, Attacked & Abused: Digital Crime Exposed" Peter Lilley examines the general problem of identity theft:

It is very easy to lose oneself on the Internet: but it is now equally possible to lose one's identity. Identity theft has become one of the boom fraud types of the last few years, and substantial media hype has ensued, directly equating this with the Internet and digital age. The simple fact, however, is that identity theft existed long before the Internet. What the Internet has done is to facilitate both the ease with which other people's information can be obtained and then utilized. Identity theft is a blissfully simple concept: the fraudster illegally acquires and uses an innocent person's personal details, credit or account information to obtain money, credit goods, services and anything else of value. All such spending or goods ultimately end up being recorded on the innocent victims credit record (as the criminal is hardly likely to pay for the goods he or she has acquired in this way). Just a note of caution, though: such a scheme will only work if the victim has a good credit record – one large case of identity theft that I investigated actually involved the details of various people being stolen who had very poor genuine credit records.

There have always been numerous ways of acquiring the required personal information to commit identity theft including:

- Mail theft – credit cards being a good option
- Theft of rubbish – you'll be amazed at what people throw away without it being shredded
- Insider access – the staff of an organization steal personal details of customers and then use them illegally
- Straight theft – steal a purse or wallet and you will usually get all of the details you need to commit identity theft

The Internet provides interesting further opportunities for criminals to collect the information that they need. One such method is through Spam – the crook sends an unsolicited e-mail and amazingly the potential victim is attracted by the amazing offer made in the e-mail, and proceeds to send his/her identifying data. Another twist on this is when false job advertisements are placed on the Internet, and the information from submitted CV's are used. The abundance of personal information that is available on the Internet (particularly in relation to US citizens) means that it is fairly easy to obtain key details in this manner. I have lost count of the number of US websites that I visit which have a pop up window offering the facility of obtaining a free copy of my own credit report. It doesn't take much imagination to see how a fraudster could use such offers to his own advantage, and obtain the credit reports of other individuals. According to the Privacy Rights Clearinghouse there are over 400,000 thefts of identity each year in the United States with annual losses of more than \$2 Billion. Identity theft is expanding at a rate of 50% per year through such techniques as this (which is a paraphrased extract from a real e-mail that I have recently received):

(Name) has several financial accounts, some of which are managed and utilized online. (Name) unfortunately used the same member name and password for all of his accounts including his Internet Service provider and bank accounts. The fraudster had obtained a considerable amount of information on (Name) and proceeded to carry out numerous transactions on (Name)'s online accounts.

Which is akin to what 32-year-old Abraham Abdallah, a restaurant dishwasher, did. In March 2001 The New York Post broke the story of this unlikely identity thief – and his even more improbable victims. The story goes that Abdallah used a high tech tool kit to steal the identities of two hundred celebrities. Well, OK I'm being slightly sarcastic: it is alleged he used the PC at his local library that had Internet access and a moth eaten copy of "Forbes" magazine "Richest People in America" list. Amongst the celebrities named in press report who had their identities stolen are Oprah Winfrey, Steven Spielberg, George Soros, Ross Perot and Ralph Ellison. The fraud began, it is believed, by Abdallah writing to credit agencies requesting confidential information on individuals using letterhead paper from brokerage house. The information that was returned appears to have been enough for Abdallah to obtain access to the stars' credit cards and bank accounts. The Forbes' Magazine was helpful as a notepad as well – it was reported that he listed on there the stars' home addresses, mobile phone numbers, social security numbers, account numbers and that old favourite, mothers maiden name. There were some hi tech elements to this extensive identity theft

episode: there was an elaborate network of post office boxes together with a voicemail system that fooled banks and credit card companies. The messages left there were picked up via Abdallah's WAP phone.

The beauty of the Internet in Identity theft is not only that relevant source details can be obtained online, but when the scam artist has sufficient information to assume the identity of an innocent victim the Internet is the ideal place to spend someone else's money.

- See also our Warning List section for comments made by Canadian authorities about "corporate and government identity theft".

FATF BLACKLIST CHANGES

On 11 October the Financial Task Force changed its list of non-cooperative countries. As it is now widely observed that the task of tracing terrorist funds has not been wholly successful and is a long-term uphill struggle, we are somewhat surprised that FATF managed to substantially reduce the number of blacklisted countries. In summary the changes are as follows:

- Countries added: None
- Countries removed: Russia (implementation of significant reforms to its anti money laundering system); Marshall Islands, Niue and Dominica (all removed because of progress made in improving their anti money laundering systems)
- Remaining on the blacklist: Cook Islands, Egypt, Grenada, Guatemala, Indonesia, Myanmar, Nauru, Nigeria, Philippines, St. Vincent & the Grenadines, Ukraine
- Still subject to countermeasures: Nauru
- New countermeasures: to be imposed on Nigeria and Ukraine if suitable steps are not taken by each country to improve their anti-money laundering regimes. Date for implementation: 15 December 2002

We cannot help but being cynical about what criteria are used to select countries for inclusion on the blacklist, what political pressures are exerted to have countries taken off the blacklist (or not included in the first place), whether the list bears any relation to the reality of the global money laundering problem (particularly as it relates to the funding of terrorism) and whether the list has any practical effects. Little wonder then that there have been growing calls for an international body to be set up that solely deals with the problem of terrorist money laundering. Just as importantly are the growing trends for launderers and terrorists to use non-traditional methods to wash funds. Examples of these are the Internet, trading in gold and the diamond market.

GLOBAL NEWS ROUNDUP

SAUDI ARABIA: Reliable information suggests that thousands of passports are being stolen from Saudi nationals and then taken to Jordan where they are sold to Iraqis for about US\$ 1,000 each document. Since the beginning of this year it is estimated that more than 5,600 stolen Saudi passports have been acquired in this way. About 5,000 of these have been stolen in Saudi Arabia and the rest have been stolen from Saudis abroad, many at European airports. Saudi authorities are tackling this problem by improving border security and enhancing travel identification documents used by Saudis.

UNITED STATES: A Las Vegas couple have been indicted on fraud and money laundering charges in a multilevel marketing scam that authorities have said could have cost about 50,000 investors more than \$30 billion. Donald Mikrut and his wife, Sue Ann Mikrut are accused of operating American Business Publications and through that entity promoting two multilevel marketing firms: Financial Independence Network Limited and Secure Independence/Partners for Life. Investors were solicited through a book that Mikrut wrote called "How to make America Strong & Wealthy, One Person at a Time"

VARIOUS: In last month's newsletter we wrote about high yield investment frauds. Judging by various stories we have been told and reports we have seen, this fraud type remains one of the most prevalent – and lucrative for criminals. In the US Michael A. Daher Sr. was sentenced to 41 months imprisonment for running a \$2 Million investment scam. As usual investors were promised guaranteed rates of return through stocks or mutual funds. In Los Angeles 28 businessmen, lawyers and others have pleaded guilty to an investment fraud that defrauded over 3000 people who thought that they were investing in high tech projects.

COLOMBIA: In late September almost 80 Colombian police officers including a former high level anti-drug official were arrested and accused of stealing more than US\$ 2 million of aid provided by the United States to combat the narcotics trade. The aid money was intended to pay for counter-drug operations but was spent on personal expenses. The United States has given Colombia more than \$2 billion over the last three years and is intending to pay about another \$500 million in the coming year.

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. KLINE MANAGEMENT GROUP

The Central Bank of Ireland has issued a warning that Kline Management Group with offices in Belgium and Japan are providing investment services without the required authorization. Kline Management Group approaches foreign investors to suggest acquiring shares in a company called Global Food Technologies. This firm appears to be domiciled at the same address as Morgan Young – we warned against this company in Newsletter 14 and quoted the address of the company as:

Avenue Louis Casa 18
CH 1209 Geneva

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

2. PIERCE WATTERS & ASSOCIATES CONSULTING LTD

The Central Bank of Ireland has issued a warning that Pierce Watters & Associates Consulting Ltd. with offices in Switzerland are providing investment services without the required authorization.

3. PRIME PACIFIC HOLDINGS LTD

The Central Bank of Ireland has issued a warning that Prime Pacific Holdings Ltd. with offices in the United States are providing investment services without the required authorization.

4. FBM VERMOGENSVERWALTUNG – AKTIENGESELLSCHAFT

The Italian authorities have warned that this firm with registered offices in Zurich has not been authorized to provide investment services in Italy in any way, including by means of distance communication.

5. BTB SERVICE s.r.l.

The Italian authorities have warned that this firm with registered offices in Bolzano has not been authorized to provide investment services in Italy in any way, including by means of distance communication.

6. CAMBRIDGE INTERNATIONAL s.r.l.

The Belgian Commission Bancaire et Financiere has issued a warning that this company, quoting an address in Milan has been providing investment services in Belgium. The Italian authorities have further confirmed that this firm has not been authorized in Italy to provide investment services so that the provision of such services outside Italy is an offence.

7. MAPLE TRUST FINANCIAL, RBC ROYAL BANK / ROYAL TRUST

The Office of the Superintendent of Financial Institutions in Canada has warned that this entity, which is not connected with Maple Trust Company, a legitimate federal trust company, is a fictional entity. Like other fictional entities previously quoted by us in Canada, it is thought that Maple Trust Financial may be connected to various Nigerian 419 frauds. As may be the following entities:

RBC Royal Bank / Royal Trust
2769 St. Clair Ave. (Avenue)
East Toronto
Ontario
M4B 1M8

However this entity is not connected with two legitimate ones: the Royal Bank of Canada or the Royal Trust Company. Because of various warnings issued in Canada about false companies using "soundalike" names the Office of the Superintendent of Financial Institutions in Canada has also issued the following general warning:

CONSUMERS AND FINANCIAL INSTITUTIONS WARNED OF IDENTITY THEFT IN ADVANCE FEE SCAMS

Over the past few months, OSFI Canada has issued several warning notices involving the use of names of legitimate Canadian financial institutions in various "advance fee" scams. Most recently, OSFI has become aware of a scam using the names of government organizations, including those of the Department of Finance, Canada Deposit Insurance Corporation and OSFI. By posing as legitimate financial institutions or government entities, scammers make it more difficult for their victims to know with whom they are dealing.

"Advance fee" scams can take many forms. Currently, the majority appears to involve classified advertisements published in newspapers, mostly in the United States. Ads often promise a guaranteed loan, even if someone had a bad credit history or no credit rating at all. They usually request an up-front fee of several hundred dollars. If money is sent, it is unlikely the promised loan will ever materialise, and the advance fee payment is unlikely to be returned.

Advance fee loans operating for criminal purpose generate millions of dollars annually in Canada.....Because scammers are using the names of legitimate Canadian financial institutions in their advertising, consumers are advised to contact the head office of a particular financial institution to verify the legitimacy of any loan offer.

OFSI asks financial institutions...to be aware that corporate and government identity theft appears to be a growing issue

8. NEW TWIST TO NIGERIAN FRAUD SCHEME

The US Treasury has issued a remarkably similar warning to that issued (and quoted above) by the Canadian authorities. However the US Treasury warning issued on 20 September particularly draws attention to government identity theft by Nigerian fraudsters. The text of the warning is as follows:

The perpetrators of Advance Fee Fraud schemes are often very creative and innovative. This scheme is commonly known as "4-1-9" fraud, in reference to the section of the Nigerian penal code that addresses this type of activity. Nigerian nationals, purporting to be officials of their government or banking institutions, will fax or mail letters to individuals and businesses in the United States and other countries.

FinCEN has recently become aware that the perpetrators are trying to provide legitimacy to the scheme by sending a letter on imitation U.S. Government letterhead with the forged signature of FinCEN's Director, James F. Sloan. In addition, this letter indicates that pursuant to the USA PATRIOT Act and an Executive Order, any money being wired into the country requires a fee to be paid, which would be applied to rebuilding the World Trade Center. The information contained in this letter is false and the letter is fraudulent. FinCEN has never issued such a letter, there is no such fee required under federal law and Director Sloan's signature was falsified.

9. LIVINGSTONE ASSET MANAGEMENT

The Belgian Banking and Finance Commission has warned against the activities of the company Livingstone Asset Management, that indicates having addresses in Geneva, Paris, Rome and Stockholm.

According to information available to the Commission, this company is approaching the Belgian public by telephone to suggest purchasing shares of Safeguard Technology, a company incorporated under the law of the State of Delaware.

Livingstone Asset Management has not been granted the authorization required to provide investment services relating to financial instruments in Belgium. In addition, the Commission has not, for this proposal, approved the prospectus required by law. According to indications received Livingstone Asset Management is trying to force interested savers into purchasing shares.

10. CHARTWELL ASSET MANAGEMENT – ADRENTACAR

In previous newsletters we have warned against the activities of various companies involved in the sale of shares in a company called AdRentaCar and other associated companies. Our last warning – issued in last month's newsletter drew attention to various companies as follows:

- Morgan Paris
- Goodman Hart & Associates
- Raymond Lloyds
- Pierce Watters

These companies have been offering for sale stock in AdRentaCar, Spantel Communications Inc. and other companies. We now have a further company to add to the list. The Belgian Banking & Finance Commission issued the following warning on 24 September 2002:

The Banking and Finance Commission warns the public against the activities of Chartwell Asset Management (18 Camille Richardson Street, St. Maarten, Netherlands Antilles), a company that may also be operating from the United States (# 2120 S. 72nd Street, Omaha, Nebraska 68124 2366, USA).

According to information available to the Commission, this company, which claims it acts on behalf of a third - unidentified - company, proposes to Belgian investors to purchase from said investors, at a rather high price, and subject to prior payment of certain costs by the seller, securities of the company AdRentaCar previously acquired by the investors through Goodman Hart Associates. The Commission wishes to emphasize that it already issued a warning on 21 December 2001 against the activities of AdRentaCar and Goodman Hart Associates.

The Commission also points out that Chartwell Asset Management has not been granted the authorization required to provide investment services relating to financial instruments in Belgium. In addition, the Commission has not, for this proposal, approved the prospectus required by law.

The Commission also wishes to stress that it is highly unusual to make such an offer conditional upon prior payment of certain costs. The Commission therefore categorically advises against accepting a proposal from that company.

11. NIGERIAN 419 FRAUD

We really would love to get through a newsletter without mentioning this fraud type, but once again we must warn against Nigerian frauds – particularly those which are variations on the theme. We particularly liked (if that is the word) the e-mail we received this month from the following gentleman, which in summary goes as follows (spelling mistakes included!) :

BE KIND ENOUGH TO ASSIST

It is with a heart full of hope that I write you, my name is Mustapha Abacha, the son of the late Nigerian President(Gen. Ibrahim Sani Abacha). During my father's reign as a president most of his activities, especially his financial involvement and transactions, I'm always involved because of my educational qualification as an economist.....

My elder brother has been apprehended by the present govt for murder case which he know nothing about just to tell you how we have been molesed by the present govt. As God may have it my mother did not move out with all the boxes, three of the boxes were left and when I heard of her problem at the airport, I smartly removed the remaining boxes. Since it appears that it was the only money left for the running of the family. With the help of a good family friend I smuggled the boxes which contains US\$60M dollars out and deposited it with a security company, of which I declared it to them as family embodiment and Antiquities.

Our main reason of writing you is for you to come to our rescue of securing this money to your country of which we will all move there to start a new life. What we need from you is to move the money from the Security Company and transfer it through a bank to your own country, as you know that we cannot present the money ourselves to a bank here in Africa as we are under surveillance.

I have agreed with my family members to give to you 25% of the total amount and also you will be a signatory to any of our investment abroad.

Just for the record (and joking apart) our serious advice is:

- 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

Police in the Italian Dolomites have set up a special unit to combat the theft of snow. Last year thieves removed snow from high in the mountains, piled it on to lorries and drove it to deprived ski resorts where it fetched about £600 per load. The Italian Police comment that they are in the middle of their investigations and have not made any arrests yet. Perhaps they are simply snowed under with information!

Rats saved a Swedish woman from a tax fraud conviction earlier this month after apparently eating the evidence. The court said it could not prove the case against the woman after she claimed that the rats had eaten her records that had been stored in an attic after her restaurant went bankrupt.

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