



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 12 – APRIL 2002

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

CONTENTS

- A MONEY LAUNDERING CERTAINTY – TRY ON-LINE BETTING
- FATF SPECIAL RECOMMENDATIONS ON TERRORIST FINANCING
- GLOBAL NEWS ROUNDUP
 - Ø Special delivery to the Yakuza
 - Ø EU directive on money laundering already obsolete?
 - Ø South Africa: one of the new centres for Nigerian fraud activity?
 - Ø Russia: cleaning up the banking system
 - Ø Ireland: the unlikely location of the country's largest money laundering operation
 - Ø United States: IRS seeks offshore cardholder information
- DUE DILIGENCE WARNING LIST
- OUR REDESIGNED & UPDATED WEBSITE

A MONEY LAUNDERING CERTAINTY? – TRY ON-LINE BETTING

Peter Lilley reflects on the largely ignored risks of money laundering and fraud through unregulated on-line casinos.

An analysis of the FATF's country blacklist (or to use its official title list of "non co-operative countries and territories") will show that one of the critical money laundering risk areas of the twenty-first century is absent. That place can be accessed by anyone: it has no formal entry requirements and is very cheap to travel in. The Internet has no geographical boundaries – and more importantly no regulation whatsoever. This new digital economy is one that has not been ignored by the criminal fraternity. Far from it: fraudsters and launderers have embraced the possibilities offered by it and turned them into certainties. There are endless opportunities offered in cyberspace – on-line betting being just one of them.

When I carried out some initial research into this aspect of cyber laundering, in March 2000 a web search using the exact phrase "Virtual Casino" produced 36,000 matches. Today an identical search gave 45,700 results. By picking just one game (blackjack) a list of over 350 virtual casinos appeared - including one that managed to combine playing blackjack with the best in adult entertainment. The total number of virtual casinos must now be in the hundreds if not thousands. These sites seek to replicate the inside and experience of playing in a real casino - and just like the real world they aim to take as much money off you as possible. It has been estimated that by this year (2002) on-line gamblers will be losing \$3 billion each year - but to lose that amount, the actual level of funds flowing through must be appreciably higher - estimates now put such revenue at \$6 billion by next year. However in truth, no one knows just how many of these sites there are, how many players are involved or the level of financial transactions. The US House of Representatives has, in various documents, described Internet gambling as a haven for money laundering and the US has sought to forbid such gaming, originally seeking refuge in the Federal Wire Act of 1960. However such attempts at prohibition bear an uncanny resemblance to King Canute's attempt to command the unstoppable waves of the sea to turn round.

The attempts by the United States to ban on-line gambling have forced legitimate gaming companies to move offshore. Thus legitimate operators become entwined with far more dubious entities in obscure offshore jurisdictions. A large number of such on-line casinos (it has been estimated up to 75% of them), are said to have their physical presence in "Caribbean locations". Having said that, a couple of sites I went on either had no physical address shown or it was almost impossible to locate. As with anything in the remoter offshore world, just because something has an address there doesn't mean that anything actually exists at that location. The governments of these countries profit handsomely from such registrations: roughly \$75,000 fees per year for sports betting sites and \$100,000 and over for virtual casinos. In 1999 it was reliably reported that the relevant jurisdictions that licence these enterprises, are raking in over \$1.5 million per month thanks to annual fees.

Obviously any one in the world can play on these virtual casinos - with no idea of what regulation (if any) exists in relation to their operation. There are additionally other risks such as credit card details being used fraudulently by the operators of such sites. Just as there is with terrestrial gambling there are wonderful opportunities for laundering funds. The FBI has in at least one previous investigation, targeted such offshore websites and their connections with wire fraud and money laundering. The jurisdictions involved were Curacao, the Netherlands, Antilles, Antigua and the Dominican Republic. Additionally there are several pending FBI investigations that link Internet gambling to organized crime (as if to reinforce the dictum that cyberspace is in many ways simply a reflection of real life). The "double whammy" of on-line casinos being dispersed across such offshore locations combined with the weak (or nonexistent) background checks in these jurisdictions make the Internet gaming market almost impossible to regulate.

Moreover, in all of this we are presuming that the relevant on-line casino does in fact "trade" - i.e. take bets from genuine customers. It strikes me (and this is hardly an original idea) that one sure-fire method of successfully laundering funds is for a launderer to claim that he operates a gambling website (but to never bother to actually do so), and thus establish a banking relationship on this basis. This gives a perfect cover for credits to come in from anywhere in the world, and payments to be made likewise. One additional complication - and advantage for the launderer - is that many on-line casinos use small offshore banks, which in turn have correspondent relationships with large US financial institutions (thus bringing us to the widely identified money laundering risks inherent in correspondent banking).

One is therefore not certain whether to laugh or cry when one finds something like the following on an on-line casino site (this is a paraphrase of an actual website entry, but its essential meaning has not been altered):

We are one of the most trusted casinos on the Internet...we operate under a license granted by (Offshore Jurisdiction named)...To play for money you first must register credit with our casino. Any funds will be played and paid out in US dollars. You can pay by:

1. Valid Credit Card

2. Wire Transfer or Bank Wire
3. Western Union Money Orders
4. Bankers Drafts, Cashiers Checks or Certified Checks
5. Personal Checks
6. You can send cash. However we do not recommend this method because it creates the wrong perception to Government officials. We operate a legitimate business and do not wish to be involved in any money laundering activity. Sending cash should be the method of last resort. We will not accept more than \$5,000 in cash *at any one time* (my emphasis).

The method you use to establish your credit is the method we will send back your winnings or any unused credit....they will either be credited back to you by a credit on the credit card used, or sent by bank wire or company check.

My advice then is, send cash in sums of just less than \$5,000 each time; play a few games (there are about twenty different to choose from) and then request on-line that your remaining credits are returned to you in the form of a cheque.

Quite what "Know Your Customer" rules apply to on-line gambling sites is open to debate. In theory, each on-line gaming site should follow the KYC rules present in the jurisdiction in which it is registered. There are various obvious weaknesses in this framework (for want of a better word) as follows:

- Most, if not all of on-line gaming sites are registered in offshore jurisdictions where anti-money laundering regulation is consistently weak. Bear in mind that on the FATF's list of non-cooperative countries and territories are (amongst others), Nauru, Niue, St Kitts & Nevis and St Vincent & the Grenadines.
- Even if the general anti-money laundering regime in a relevant location is adequate, it is highly unlikely that there are any relevant regulations regarding on-line casinos, particularly in respect of customer due diligence.
- Added to these factors is the lack of transparency which is a key element in such offshore havens.

Thus, in practice, based on a sample of offshore casinos we have visited (purely for research purposes, you understand) the general KYC procedures seem to be that casino operators will take whatever a customer says at face value and do very little – if anything – to validate such information.

As a potential money launderer we particularly were drawn to a gaming site operating from a PO Box in Antigua. This site accepts payments by bank cheque, bank draft, American Express money order – or good old cash. Cash payments are fine – as long as they are sent by registered mail. Then the site helpfully delivers your remaining account balance when requested by "Private courier anywhere in the world, free of charge" or alternatively will send "any payment by registered mail completely free of charge".

Combined with this anonymity are the attractions of remote access to place bets (and thus move funds) and the encrypted data being used. Thus whilst law makers, regulators and law enforcement bodies belatedly focus on closing down the money laundering loopholes which still exist in the "physical" world, their opponents are making the optimum use of what is available in cyber space. Any one for a bet as to who is winning?

FATF SPECIAL RECOMMENDATIONS ON TERRORIST FINANCING

In the aftermath of 11 September FATF issued a two-page document giving "Special Recommendations on Terrorist Funding" outlining eight key recommendations. On 27 March 2002 an additional set of guidance notes were issued to give further advice on how to implement the recommendations. This new and additional information contains the following important observations:

1. Each country should ratify and implement relevant UN instruments: the guidance notes provide full details of the six elements of the UN convention and Security Council Resolutions
2. Each country should criminalise the financing of terrorism, terrorist acts and terrorist organizations: The guidance notes give additional information of exactly what this involves, including the key observation that "jurisdictions should ensure that terrorist financing offences are predicate offences even if they are committed in a jurisdiction different from the one in which the money laundering offence is being applied"
3. Freezing & confiscating terrorist assets: the three key elements of freezing, seizing and confiscating are further explained and defined
4. Reporting suspicious transactions relating to terrorism: the two key elements of suspecting and having "reasonable grounds to suspect" are further explained. Additionally the types of entities which should report such suspicions are stressed: not only banks but also non-bank financial institutions (which, as a minimum, should include bureaux de change, stockbrokers, insurance companies and money remittance/transfer services)
5. International Co-operation Further information is given regarding the five elements of this recommendation as they apply to each jurisdiction, which are: Exchange of information through mutual legal assistance mechanisms; exchange of information other than through mutual legal assistance mechanisms; having specific measures to permit the denial of "safe haven" to those involved in terrorist financing; having procedures to permit extradition; jurisdictions should have provisions or procedures to ensure that "claims of political motivation are not recognised as a ground for refusing requests to extradite persons alleged to be involved in terrorist financing"
6. Alternative Remittance this recommendation attempts to tackle the difficult area of value transfer systems such as the Black Market Peso Exchange, hawala or hundi systems and other methods prevalent in China and East Asia. The notes give clarification of the three major elements of this recommendation: Jurisdictions should require licensing or registration of those providing such services; Such systems should be subject to FATF recommendations: Jurisdictions should be able to apply sanctions on such systems if they fail to obtain a licence/or register and fail to comply with relevant FATF recommendations
7. Wire Transfers The three elements of this recommendation have a direct impact on the operations of financial institutions, and in our opinion should be viewed as, at the very least, best practice guidelines. The three aspects are that jurisdictions should require financial institutions to:
 - include originator information on funds transfer sent within or from the jurisdiction
 - retain information on the originator of the funds transfers, including at each stage of the process
 - examine more closely or monitor funds transfers when originator information is not available
8. Non-profit organizations This recommendation consists of two key elements: Jurisdictions should review the legal regime of entities, in particular non-profit organizations, to prevent their misuse for terrorist financing purposes and secondly non profit organizations should not be used to disguise or facilitate terrorist funding and thus escape asset freezing measures.

GLOBAL NEWS ROUNDUP

JAPAN: In our last newsletter (Newsletter 11 – February 2002) we reported on the global threat posed by the Japanese Yakuza. Their influence is many faceted: but perhaps none more bizarre than the problems recently discovered at Japan's postal agency. A survey of 5,000 senior postal staff uncovered that 344 post offices (including 50 in Tokyo) were giving "special treatment" to mail sent by (or addressed to) known gangsters – and had been doing so for many years. The organized crime bosses had previously complained that their mail arrived "dirty, scuffed or late". Eager to please this important group of customers, postal workers placed relevant mail in unofficial specially marked bags so that it could be given the respect and care it obviously deserved. Post office management are now working with police on anti-mob measures so that postal staff can handle Yakuza related mail "with courage"

EUROPEAN UNION: Even though the EU directive to combat money laundering has only recently been amended, it has come under attack for being ineffective. Gerhard Schmid, a vice president of the European Parliament has argued that it must be revised again. He has called for the extension of the law against money laundering to include the disguising of legally acquired money

if such funds were used to finance crimes. He also called for a register of all EU bank accounts, the registration of banks in the Channel Islands and a ban on all correspondent accounts with shell banks. He also observed that sooner or later the United States would demand a tightening up of EU directives. Mr Schmid's information is that Jersey, Guernsey, the Balkans and Russia are all weak points in the fight against money laundering and additionally links with offshore banks should be monitored far more closely.

SOUTH AFRICA: During March the 29 year old Nigerian co-owner of a telecommunications company, Global Net was arrested in Durban. The large investigation which preceded this arrest focused on various alleged crimes: a money laundering scheme for crime syndicates involving drug dealing in the Netherlands, Colombia and Venezuela; Cellphone fraud involving thousands of rands through placing calls on innocent peoples phones and activating stolen phones together with involvement in 419 frauds. Earlier in March another Nigerian involved in "Royal Net Communications" was arrested: he is believed to be the mastermind of a large series of 419 frauds.

RUSSIA: The Russian Government's Financial Monitoring Committee (FMC) is investigating thousands of suspicious transactions and compiling its own list of countries suspected of harbouring Russian money (which currently in draft form contains 54 jurisdictions). Formed on 1 February 2002 the FMC has already received over 40,000 reports about suspicious transactions – and is determined to do all it can to get Russia removed from the FATF country "blacklist". Viktor Zubkov, the task force's head commented in March that "we already have a number of companies and individuals who we want to question because they are, in our opinion, laundering dirty money". However a FATF delegation which visited the country in March commented that Russia was still not taking sufficient measures to combat money laundering – whilst the current laws were being implemented properly, they did not include casinos or investment funds. Realistic observers believe that Russia will not be removed from FATF's blacklist until February 2003, at the earliest.

IRELAND: Could it only happen there? In February a court was told that the largest money laundering operation ever was carried on next door to a Garda (Police) station at Dromad, near the Louth-Armagh border. Dromad Enterprises operated as a bureau de change (with a turnover of £17 million a year) and as a private bank, handling up to £60 million for 150 customers. Whilst the business had many legitimate customers it was also frequently visited by couriers from Dublin organized crime groups who delivered upto the equivalent £100,000 in Irish Punts at a time in black plastic bags for laundering into sterling.

UNITED STATES: The IRS have recently been making various moves to obtain details from credit card issuers concerning US taxpayers who hold credit cards issued by banks in various tax havens. In late March the IRS went to court in an attempt to get Visa International to release records of taxpayers who have cards issued by banks in locations including Antigua and Barbuda, the Bahamas, The Cayman Islands, Hong Kong, the Isle of Man, Liechtenstein, Luxembourg and Switzerland. Whilst such ownership of cards is not illegal, US taxpayers are required to report ownership of any offshore bank accounts: but few do. The IRS estimate that 2 million Americans may have such cards but only 100-200,000 are reported to them. In October 2000 the IRS won a court order authorising it to serve summonses on American Express and Mastercard.

DUE DILIGENCE WARNING LIST

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

1. HASSO P. NERLICH ASSET MANAGEMENT

Authorities in Luxembourg have highlighted this company which is apparently offering customers the opportunity to invest in bonds. The company has not been authorized to offer such services in or from Luxembourg

2. ADV ADVANTAGE SA – GLOBAL ASSET MANAGEMENT

24 Avenue de la Liberte
Luxembourg

Authorities in Luxembourg have also highlighted this company which is apparently offering customers investments in high yield bonds. The company has not been granted the required authorization to offer such services in or from Luxembourg.

3. VARIOUS COMPANIES – WORLDWIDE

The Central Bank of Ireland have issued warning notices about various (unrelated) companies which do not have the appropriate authorization(s) to operate in Ireland. The firms noted are:

- AVID INVESTOR, INC. (Hong Kong & the Cayman Islands)
- CLANVALE SECURITIES SA (Venezuela)
- CLEARING SERVICES (Spain)
- CRANLEY & ASSOCIATES S.L. (Spain)
- J.P.TURNER & COMPANY LLC (USA)
- MILLENNIUM FINANCIAL LIMITED (Uruguay, Brazil, Switzerland, Singapore & Mexico)
- MORGAN PARIS & COMPANY (Spain)
- POWERS BOOTH LIMITED (Austria)
- ROYAL CAMBRIDGE SECURITIES CORPORATION (Panama)

4. VARIOUS COMPANIES – JAKARTA, INDONESIA

The Indonesian Capital Markets Supervisory Agency (Bapepam) has issued a general warning to investors about unregistered stockbrokers who appear to be operating in Indonesia or claim to be operating from Indonesia. Three companies have been specifically named:

- MENDES PRIOR EUROPE
- JF KIDWELL
- PFEIFFER GALLAND

5. VARIOUS LINKED COMPANIES

The Belgian Banking & Finance Commission have warned against various companies that are offering to purchase securities that were previously sold by associated companies. The companies involved are:

- ALPHA MANAGEMENT
13 Camille Richardson Street
St Martin
- WEDGEWOOD ACQUISITIONS
Schottenfeldgasse 51
1070 Vienna
Austria
- TRANS-NATIONAL SECURITIES TRUST SA
World Trade Center
Leutschenbachstrasse 95
8050 Zurich
Switzerland
- PRICE RICHARDSON
31st Floor
Citibank Tower
Citibank Plaza
8741 Paseo de Roxas
Makati City 1200
Philippines

6. CHASE TRUST BANK

The US Office of the Controller of the Currency has issued a warning about this entity, which is not associated in any way with Chase Manhattan Bank of New York (or any of its subsidiaries and/or associates). Chase Trust Bank is operating without authorization and gives an address of:

2706 Wisconsin Avenue
Washington DC
United States

7. VARIOUS CANADIAN ENTITIES

The Office of the Superintendent of Financial Institutions in Canada has issued warnings about the following entities, which are non-existent "banks" linked to Nigerian frauds:

- BANK OF CENTRAL ATLANTIC
- KANADIAN WESTERN BANK (not connected with Canadian Western Bank, a legitimate bank)
- FIRST SECURITY FINANCIAL SERVICES

The OSFI has also issued a general warning about "Nigerian Advance Fee Frauds" noting that fraudulent communications are now coming from other countries such as South Africa and Sierra Leone, as well as Nigeria. OFSI comment that "during the past few weeks OSFI has seen an increase in reported advance fee scams".

8. TCF NATIONAL BANK LETTERS

TCF National Bank in Minneapolis, MN, USA (which is a legitimate financial institution) has advised that certain "confirmation of funds" letters, issued by the bank's Arlington Heights Road branch office were issued without the authority of the bank. These letters, which are also referred to as "Bank Capability Letters" refer to transactions involving Medium Term Notes/Medium Term Senior Subordinated Bank Debentures in amounts of \$500 million and more, in total or per tranche. These letters have no value.

OUR REDESIGNED & UPDATED WEBSITE

We have recently completely redesigned and updated our website www.proximalconsulting.com, with the aim of making it both more informative and easier to navigate. The key elements of the site are:

- Details of our range of services including Due Diligence reports, Asset Tracing and Recovery, Investigations, Training & Education and Compliance & Assurance projects.
- A new section, [Publications by Peter Lilley](#) provides information about "Dirty Dealing: the untold truth about global money laundering". Additionally this section provides advance notice of Peter Lilley's new book on e-crime, fraud and risk in the digital age which is to be published on a worldwide basis in September 2002 by Kogan Page. This new section also includes links to various articles written by Peter on money laundering and associated topics.
- The existing [Money Laundering & Terrorism](#) page has been expanded to include various links to relevant documents on this subject, including the complete list of terrorist related individuals and organizations as issued by the US authorities.
- The [Newsletters](#) page contains an index of all of our previous newsletters. You can now also download all of our previous newsletters in PDF format
- The [White Papers](#) page has been updated and the accessing and downloading of White Papers has been made far easier. Included in this section of the site are nineteen White Papers on various topics relating to money laundering and business crime, including a new overview paper "What is Money Laundering?"
- The [News](#) section is updated on a real time basis and contains relevant headlines of current stories that then link to the full text of the article.
- We have created a new section, the [Proximal Info Center](#) that is split into five separate sections: Money Laundering, the A-Z of Money Laundering, Know Your Customer, Country Risks and Investor Alerts. Each section provides further information and links to each subject. The A-Z of

Money Laundering, for example, provides a useful glossary of money laundering and related terms. We are still developing this area of the site and new sections planned include a section on Digital Crime and a country by country money laundering risks index

We hope you find the site helpful and informative – news of additional updates and developments will be included in future newsletters. Updates due by 12 April include links to all relevant FATF and US government documents together with the latest examples of Nigerian 419 letters.

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