



◆
E-MONEY
AND CYBER
LAUNDERING:
VIRTUAL DIRTY
DEALING

◆
GLOBAL
CORRUPTION
BAROMETER
FOR 2006

◆
FOCUS ON
FRAUD:
NIGERIAN 419
FRAUD

◆
TRAVEL
SCAMS

◆
AND THEN
THERE WERE
NUN

◆
SERVICE
DIRECTORY
&
CONTACT
DETAILS

■ Welcome to the March/April 2007 issue of the Proximal Consulting Review. Thanks to all our readers for their positive and encouraging feedback regarding the first edition, your comments are always welcome. In this issue we bring you reports on the threat of cyber laundering, Nigerian 419 fraud, and a number of travel scams affecting unsuspecting holidaymakers abroad. In addition, we are delighted to announce the launch of our new and improved website, www.proximalconsulting.com. The new-look site includes KYC and AML mini-sites, the latest information concerning our new and existing services and much more.

E-MONEY & CYBER LAUNDERING: VIRTUAL DIRTY DEALING by Peter Lilley

■ The Internet and the continuing development of e-money systems not only transforms the way we do business across the world but also, if it has not already happened, provides considerable scope for the laundering of funds in cyberspace. The customer and transactional model for e-money providers is a simple one, and is similar to a credit card provider. A customer makes an application for an e-money account, usually on-line, by providing personal information that can be verified by the provider. This is where KYC (Know Your Customer) procedures come into play. The provider should verify the identity of the customer before allowing any account or relationship to be opened. If an e-money account is established then the customer can finance it by a variety of methods – if the provider is a legitimate one this is usually by drawing funds from an existing bank account. However, we have seen some less scrupulous providers accepting cash or money order payments. We have also (purely for experimental purposes) been able to open an e-money account with a smaller provider by supplying completely fictitious information which was not verified or validated. If e-money providers do not have robust KYC procedures to check their prospective customers, the consequences are blindingly obvious. A secondary concern is that on-line customer applications, even with suitable KYC checks, are a fertile breeding ground for criminals to commit identity fraud. Know Your Customer checks will not usually identify applications where the customer details being used are real but stolen.

For e-money to be an accepted payment method, the provider needs to have merchants. Having an e-wallet is useless unless the website the customer wants to use it at accepts it. Thus the e-money provider signs up merchants (as many as possible) who are predominantly, if not exclusively, companies transacting business on the Internet. And this is where the major difficulties begin: there are a range of worrying alternate merchant activities that may be taking place.

The merchant could be a front for organized criminal activity: the merchant operates a real business such as an on-line casino with actual customers, but simultaneously uses it as a front to co-mingle criminally obtained funds and thus uses the e-money provider to distribute these funds. The criminal merchant could claim to operate a real business but in reality has no genuine customers: the merchant uses the e-money provider to launder and distribute dirty money. The merchant could be operating an on-line business, but that in itself is conducting criminal activities – for example, the casino that never pays out and just rips off players.

It should also be appreciated that all of the above basic

examples have other variations and it is highly likely that a criminal merchant will use sophisticated methods to disguise their true activities so as to make their actual e-money transactions appear genuine.



The added complication is that it is not only money launderers who could make use of e-money systems; what about a merchant who is acting as a front for terrorist funding? A terrorist group could operate a real business on the web but co-mingle terrorist funds with real transactions, and use the e-money system to both generate funds from sponsors and distribute funds to terrorist operatives. A terrorist group could also establish a phoney website – doing no real business – and use this front to collect and disburse funds. A third variation is that a terrorist cell could set up a fraudulent website (one which scams its users) and then use the money obtained in this way to support terrorist activity, using the e-money system to move funds.

Whilst e-money systems have limited use as a money laundering placement tool (unless the provider accepts inward cash payments), the potential for them to be used in other stages of the money laundering or terrorist financing process is considerable. Additionally the development of peer to peer payments through such systems amplifies these risks. Peer to peer transfers are simplicity itself: I have an e-wallet and I want to transfer value to a friend or family member who also has an e-wallet – and the transaction is as simple as clicking my mouse. The risks are clear: such a system has been described overall as being too close to real cash for comfort. Imagine I am a money launderer in Brazil with an existing bank account that is used to launder drugs money: I draw money out of that account via the Internet to my e-wallet; I then transfer value to an associate in the US (or Europe – or potentially anywhere around the globe); he then transfers the funds to his bank account. The beauty of this being that when the funds hit the associate's account the transaction will show up as being from the e-wallet provider company and not the original bank in Brazil. If I wanted to complicate things (and leave a complex trail) I would make sure that the funds are transferred numerous times between various e-wallets.

In the end, e-money has no country boundaries, has no requirements for face-to-face meetings and there are no professional advisors asking awkward questions about source of funds. Indeed, there are very few, if any controls present that can halt the washing of dirty money in cyberspace in this way.

TRANSPARENCY INTERNATIONAL PUBLISHES ITS GLOBAL CORRUPTION BAROMETER FOR 2006

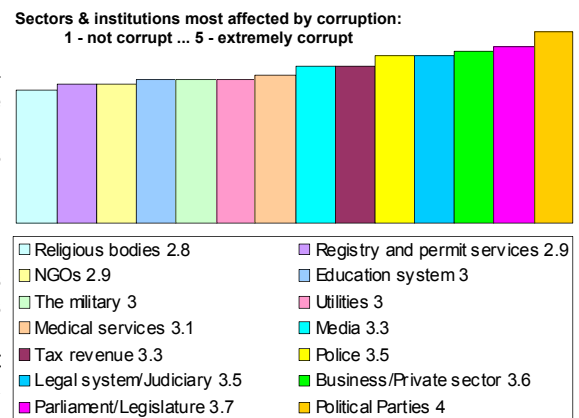
On 7 December 2006, the global civil society organisation Transparency International (TI) published its annual Global Corruption Barometer (the Barometer), which explores how corruption affects ordinary people. The Barometer provides an indication of both the form and extent of corruption, from the point of view of citizens around the world. The 2006 Barometer explores petty bribery and asks people about their opinions regarding which sectors of society are the most corrupt and which spheres of life are most affected by corruption. TI believes that people's perceptions are an indicator of the success of anti-corruption policies and initiatives, playing a vital role in anti-corruption efforts. The Barometer 2006 reflects the findings of a survey of 59,661 people in 62 low, middle and high-income countries that was carried out on behalf of TI by Gallup International, as part of its Voice of the People Survey, between July and September 2006. According to TI, the Barometer 2006 is one of TI's key global tools for measuring corruption, and the public opinion focus complements the Corruption Perceptions Index (CPI) and Bribe Payers Index (BPI). The CPI and BPI reflect the opinions of experts and business leaders, and focus on the perception of public sector and political corruption, and the supply side of bribery, respectively.

The Barometer 2006 found that Albania, Cameroon, Gabon and Morocco were the countries most affected by bribery; while Switzerland and the UK were two of twenty-five countries found to be least affected:

Table 1: Countries most affected by bribery

PERCENTAGE OF RESPONDENTS THAT HAVE PAID A BRIBE IN THE LAST 12 MONTHS	> 40%	Albania, Cameroon, Gabon, Morocco
	16 - 40%	Bolivia, Congo-Brazzaville, Czech Republic, Dominican Republic, Greece, Indonesia, Kenya, Mexico, Moldova, Nigeria, Paraguay, Peru, Philippines, Romania, Senegal, Ukraine, Venezuela
	6 - 15%	Argentina, Bulgaria, Chile, Colombia, Croatia, Hong Kong, India, Kosovo, Luxembourg, Macedonia, Pakistan, Panama, Russia, Serbia, Thailand
	< 5%	Austria, Canada, Denmark, Fiji, Finland, France, Germany, Iceland, Israel, Japan, Malaysia, Netherlands, Norway, Poland, Portugal, Singapore, South Africa, South Korea, Spain, Sweden, Switzerland, Taiwan, Turkey, United Kingdom, USA

Source: Transparency International Global Corruption Barometer 2006



According to the Barometer 2006, bribes are most commonly paid around the world to the police, and are substantially more frequent than to other services. TI highlights the enormous concern this result presents when viewed alongside the sector identified as the third most common recipient of bribes – the legal system and judiciary.

The Barometer 2006 provides data on how corruption is perceived to affect public sectors and institutions. TI's findings in this respect confirm that political parties and parliament/legislature are considered to be the most corrupt with the business/private sector and police a close second:

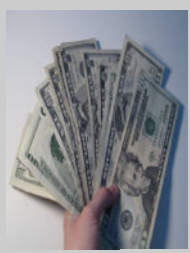
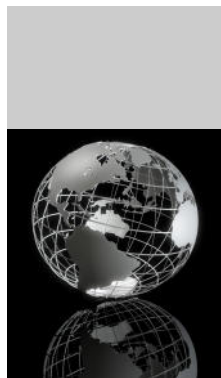
The Barometer 2006 found that "the majority of people around the world have a poor opinion of their government's anti-corruption efforts", indeed fifteen percent of the public worldwide said they believe that not only is government not effective in its anti-corruption work, but that government actually encourages corruption. In support of this finding, political life emerged as the sphere of life thought to be most affected by corruption, followed by the business environment and, of much less concern, personal and family life. Corruption was thought by those surveyed to have the greatest affect on political life in Bolivia, Cameroon, Greece, South Korea and Taiwan:

Table 2: Corruption affected political life to a large extent

CORRUPTION AFFECTS POLITICAL LIFE TO A LARGE EXTENT	> 70%	Bolivia, Cameroon, Greece, South Korea, Taiwan
	51 - 70%	Albania, Argentina, Bulgaria, Chile, Croatia, France, Gabon, Hong Kong, Indonesia, Israel, Italy, Kenya, Macedonia, Mexico, Nigeria, Peru, Paraguay, Philippines, Poland, Portugal, Romania, South Africa, Russia, Senegal, Spain, Turkey, UK, Ukraine, USA
	31-50%	Canada, Colombia, Congo-Brazzaville, Czech Republic, Dominican Republic, Fiji, Germany, Iceland, India, Japan, Kosovo, Moldova, Morocco, Pakistan, Panama, Serbia, Singapore, Thailand, Venezuela

Source: Transparency International Global Corruption Barometer 2006

The Barometer 2006 concluded that corruption remains a problem worldwide and there is a widespread perception that the authority vested in institutions that ought to represent the public interest is being abused for private gain. Bribe-paying was found to most affect the poorest countries, in other words those who can least afford it. The Barometer 2006 states that it is in these countries, that the misuse of public funds does the greatest harm to the money available for clean water, schools and health care. TI challenges political leaders to prove that they are not actually fuelling corrupt practices, but are playing a genuine part in efforts to enhance transparency, accountability and integrity in societies around the world. The full Barometer 2006 report is available for free download at www.transparency.org.



FOCUS ON FRAUD: NIGERIAN 419 FRAUD

■ Fraudsters and scam artists will stop at nothing when it comes to parting you from your cash. Some schemes have been around for years, while others have evolved or emerged more recently. The Office of Fair Trading (OFT) estimates that consumers in Britain lose £1bn a year to cons. In this issue of the Proximal Consulting Review we focus on Nigerian 419 Fraud.



Research has shown that victims of Nigerian 419 e-mail scams are losing an average of £30,000 each; indeed this form of fraud alone is reported to be costing the UK £150 million annually. According to the research group Chatham House, poverty in Nigeria has led to a marked growth of criminal networks, which have become a "large and pressing problem" in the UK.

Nigerian 419 scams are named after Section 419 of the Nigerian penal code which deals with fraud. They usually arrive in the form of a letter or fax, although e-mail is now being used as well, but all essentially offer the same – to pay you thousands or, in some cases, millions of pounds for allowing a large amount of money to be paid into your account in return for a share, commonly 30-40%! Before this can happen however, you are asked to pay an up-front fee (this type of scam is also called "advance fee fraud" for this reason). Upon receipt of this fee, the correspondent offering the unbelievable deal disappears, along with your money. If you have disclosed your bank account details along the way, your bank account will be stripped into the bargain.

The names and addresses of recipients are taken from business directories which are widely sold on the open market in Lagos. Typically the writer claims to be a senior civil servant (The Nigerian Petroleum Corporation being a favourite employer), however Nigerian 419 scams are a constantly evolving threat - some of the more recent and topical 419 scams include:

- A young person orphaned by the tsunami disaster asking for help in moving their parents' millions out of an overseas bank account.
- A war reporter who has unearthed Saddam Hussein's missing millions and needs to deposit them in your account.

The 419 letters will sometimes have deliberate spelling mistakes and be written in poor handwriting to appear more "authentic" and so appeal to the reader's sense of compassion and pity (as well as greed). Most 419 scam letters share various key factors:

- There is a sense of secrecy and urgency.
- The recipient is enticed to travel to Nigeria or a bordering country.
- All communication is dealt with by fax or letter; however the use of e-mail is increasing.
- Various details are requested from the recipient such as blank letterheads, invoices and bank account details.
- There are normally claims of strong ties to Nigerian officials or the senders are high ranking officials themselves.

We have compiled some general tips for avoiding Nigerian 419 Fraud:

- 1 If you are targeted, recognise the 419 for what it is – an attempt to defraud you. Any offer that looks too good to be true is. You will never get anything for nothing so do not let anyone (however plausible) persuade you otherwise.
- 2 Do not reply to the letter/e-mail, even to say no – by doing so you provide the fraudsters with your signature.
- 3 Never under any circumstances give out your personal details.
- 4 Never pay anything up-front to anybody for any reason.
- 5 Never agree to meet with the people sending you letters.
- 6 Never expect any help from the Nigerian government.
- 7 Never travel to Nigeria (or nearby countries) – either to pursue a tempting offer or the people who have ripped you off.
- 8 Report any losses to the relevant authorities. If the letters arrive in the form of an e-mail, contact the Internet service provider from which the scam e-mail originated. Your e-mail should be addressed as: abuse@[ISP name] e.g. abuse@hotmail.com.
- 9 Unless you are almost uniquely fortunate never expect to recover any money you have lost.

For further information regarding Nigerian 419 Fraud and other West African scams please see Proximal White Paper 13 – Nigerian & West African Fraud available at <http://www.proximalconsulting.com/whitepapers/whitepaper13.htm>.

TRAVEL SCAMS

■ If you're about to head off to foreign climes, be it for business or pleasure, read the Proximal Consulting Guide to Travel Scams.

Security Scam

As if delayed flights, queues and airline food were not enough to contend with when jetting off abroad, travellers also face the possibility of being scammed *before* they even set foot on the plane. Airport security checks provide pairs of crooks with ample opportunity to make off with your brand new digital camera, mobile phone or wallet. As you place your valuables on the conveyor belt and wait patiently to pass through the metal detector, the first person passes through unchallenged whilst the second sets off the alarm. As the person in front of you slowly empties their pockets of change, keys, chewing gum and cigarettes, the first person has casually helped himself to your belongings which have already passed through the x-ray machine.

Hotel Hustle

Tired and jetlagged, you are looking forward to relaxing in your hotel room when the telephone rings. It is hotel reception, apologising for any inconvenience but asking you to verify your credit card details. You willingly oblige, thinking only of the contents of the mini-bar and what you are about to order from room service. Except the phone call was not from the hotel receptionist; it was a trickster who now has all the information needed to max out your credit card while you sleep.

Shopping Swindle



Making the most of the good exchange rate, you decide to invest in the latest electrical gadget which costs half the price it does back home. The shop assistant carefully packages it for you (all the better to survive the return journey). It is only when you arrive home and unwrap your new toy that you realise your top-of-the-range product has been replaced with something cheap, inferior and most probably faulty.

Restaurant Rip-Off

You are in "one of the finest restaurants in town", or so the guide book tells you. You fancy treating yourself to one of the live lobsters (priced by weight) on offer – well, you are on holiday after all! Unfortunately you failed to check the exact price before the meal and now you have been presented with an extortionate bill which cannot possibly be right. And it is hard to argue your case when you have swallowed the evidence.

Tyre Trick

If you manage to survive the foreign drivers, unfamiliar road signs and cheap rental car, you may think that driving abroad is a piece of cake. But then another motorist pulls up alongside you, indicating that you have a flat tyre. As you pull over to inspect the damage, the kindly driver stops too in order to help you. Whilst you are checking the vehicle, your helper is surreptitiously pocketing your wallet, passport and anything else of value from the front seat before driving off with a cheerful wave.

AND THEN THERE WERE NUN

■ A whole convent of 55 nuns has gone into hiding after amassing huge debts. The nuns fled their nunnery on the Greek-Bulgarian border after their knitting business crashed leaving debts of around 750,000 EUR. According to media reports, the sisters travelled to fashion shows abroad to see the latest knitting designs – this was one factor which contributed to their huge debt. The nuns have taken refuge in another convent whilst the Greek Holy Synod is trying to persuade them to come out of hiding and to sort out their financial problems. Hopefully the sisters will not make a habit of it!



SERVICE DIRECTORY



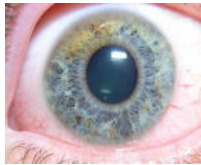
NEWSLETTER INFORMATION

Can you afford to be without this critical intelligence? You can subscribe to this newsletter and download all previous issues from our website. *Issue 2 of the Proximal Consulting Review is brought to you by Peter Lilley, Jane Smith, Alison Keyzor, James Lilley, Valerie Dalgleish & Jo Mason.*



DUE DILIGENCE BACKGROUND REPORTS

One of our core business areas is providing global due diligence background reports on individuals and/or companies that are structured to provide focused intelligence in a cost efficient manner and in accordance with your needs. More importantly, our many years of experience in this field ensure that the legal and regulatory obligations of our clients in regard to due diligence are met. We ensure that you, as our client, are not exposed to reputational, operational, legal or concentration risks. Additionally, we have a wealth of experience in providing **MERCHANT BACKGROUND CHECKS**.



KYC DUE DILIGENCE WARNING BULLETIN

We publish a monthly KYC Due Diligence Warning Bulletin which details critical intelligence on a worldwide basis concerning individuals and companies that are known to be involved in fraudulent and/or money laundering activity. The annual subscription is £250 and includes a monthly updated fully searchable database that incorporates all entries from the first bulletin, published in February 2003. This database now contains over 5,000 warning entries.



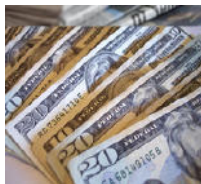
COUNTRY REPORTS

Our country reports provide you with reliable and credible advice on country risks, a further invaluable tool for staying ahead in the fast-moving international business environment of today. We analyse national and local risks in each country and provide a detailed examination of political, general business, money laundering and corruption factors.



AML TRAINING

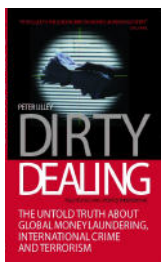
We provide a full range of high quality Anti Money Laundering training and prevention services. These include: creating and devising KYC and AML procedures, designing and delivering customised AML training packages, producing definitive AML training material (including client-specific training films), evaluating your AML "defences" to ensure regulatory compliance together with providing ongoing AML advice and guidance either on a general level or relating to specific events.



ASSET TRACING & OTHER INVESTIGATIONS

We are able to provide our clients with proven methodologies and the latest tools for investigation, evidence gathering and asset location to freeze and seize funds. Our in-house abilities together with our global network of contacts ensure that we are able to provide a worldwide coverage. Additionally, we have substantial experience in developing overall winning strategies in asset tracing projects and other types of complex and high profile investigations.

FURTHER READING...



DIRTY DEALING

The third completely revised edition of Peter Lilley's acclaimed book on money laundering was published during 2006.

One of "Director" magazine's business books of the year.

"Entertaining, well written & well presented"
The Irish Times

www.dirtydealing.net



HACKED ATTACKED & ABUSED

"Hacked, Attacked & Abused" exposes the full extent of digital crime and how to avoid falling victim to it.

"This book is an excellent exposé of digital crime stemming from Peter Lilley's own expertise in the field of prevention, detection and investigation of global business crime and money laundering"

-*Asian Voice*

CONTACT US

UK Office

2 Pelham Court
London Road
Marlborough
Wiltshire
SN8 2AG
United Kingdom

Telephone: +44 1672 516725
Fax: +44 1672 516759
E-mail: enq@proximalconsulting.com
Website: www.proximalconsulting.com

Swiss Office

Rue du Rhone 14
1204 Geneva
Switzerland