



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 18 – APRIL 2003

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

CONTENTS

- Identity Fraud – a media led false panic or a serious global problem?
- Fraud, Conceptual Art or Administrative Terrorism?
- Money Laundering via Premium Rate Phone Lines
- Global News Roundup:
 - Two “high yield” investment scams in the UK
 - Calvi – the theories continue
 - The two Albertos jailed in Spain
 - War Homeland Security scams
 - Nigerian 419 Internet auction frauds
 - You’ve won the Dutch Lottery!
 - US Technologies CEO faces further charges
 - FinCEN fines Western Union
 - Australia’s Commonwealth Bank hit by fictitious website
 - The problem of stolen cars in Russia
- The Final Word
- Proximal Consulting Service Directory

IDENTITY FRAUD – A MEDIA LED FALSE PANIC OR A SERIOUS GLOBAL PROBLEM?

Peter Lilley returns to the subject of Identity Fraud in the light of recent media coverage.

In Newsletter 15 (October 2002) we led with a story on “Identity Fraud” reprinting a section from my book “Hacked, Attacked & Abused: Digital Crime Exposed” (Kogan Page). Since then the problem of Identity Fraud has become one of the favourite media issues of its kind. Are these frequent scare stories justified – or is the apparent panic exaggerated?

What is certain is that whilst the risks posed by identity fraud and theft are real ones, they are not necessarily new. However, because of the higher profile of "identity theft" as a fraud categorisation, more meaningful figures relating to the level of this problem are emerging. Before examining these figures it is worth observing that I first dealt with what would now be termed an identity theft case over fifteen years ago when the identities of real people were stolen and used to apply for bank accounts and credit cards. In that particular case over 150 identities were stolen and banking facilities obtained by the criminals behind the scam.

The current wave of interest has been generated by fairly authoritative reports and estimates such as the following:

- In 2002 a UK Cabinet Office report concluded that identity fraud/theft is a serious and growing problem that costs the UK more than £1.3 billion a year (which may be more of a problem than it first appears because, ironically there is no criminal offence of identity fraud in the UK)
- The UK National Criminal Intelligence Service (NCIS) in a report issued in February 2003 concluded that "there is no comprehensive data on identity fraud. Intelligence is patchy and not always reliable.....this makes it difficult to reach firm judgements"
- Notwithstanding this fact NCIS think that: identity theft underpins much serious and organized crime; identity theft cuts across most criminal sectors; serious and organized criminals have little difficulty obtaining false identity documents and there are "significant" intelligence gaps in respect of how identity fraud is successfully undertaken
- In the UK it has been reported that identity theft cases have doubled to 75,000 in two years
- On March 2, the UK "Sunday Times" reported that Scotland Yard detectives are investigating more than 30 websites that are selling false documents
- A spokesman for the US Attorney's office commented in March 2003 that identity theft was "very frequent" and "out of control"

And as if all of this wasn't worrying enough NCIS also warned in March 2003 that criminal gangs, based mainly in Nigeria, are infiltrating Britain's high street banks and call centres, raiding accounts and stealing identities.

Identity theft is a notoriously difficult problem to solve: because in very simple terms individual consumers cannot totally guard against the theft of their details, and organisations can never be certain that they are dealing with the "real" person without conducting effective due diligence enquiries. However we suggest the following guidelines (albeit that even if you follow all of these to the letter it does not guarantee that you will not be a victim)

CONSUMERS

- Beware of "bin raiding" – the theft of your rubbish. Shred, burn or completely destroy all material that shows your name, address or any other information that contains information that can be used by an identity thief. Even though they may seem to be both innocuous and annoying, also shred "pre-approved" credit offer mailings that contain personal information
- Reduce access to your personal data: do not carry extra credit cards, passport, driving licence, SSN card (US) or any other similar documents unless you have to
- Arrange to collect new cheque books and plastic cards from your bank – thus reducing the chance of them being stolen in the post (which is still a massive problem area)
- Passwords and PINS: do not use common numbers, consecutive numbers, your date of birth or any series of numbers that could be easily identified by a thief. Never write passwords and PINS down (particularly never write them down on the relevant plastic card or bank document itself!!)
- Don't allow your plastic cards out of your sight – you may be unpopular in restaurants but so what – you're the customer!
- Handle information wisely – review your credit card, bank and telephone bills for unauthorized use; store important documents safely.

ORGANIZATIONS

- Be aware that criminal gangs do attempt to 'plant' staff so that they can steal confidential information. A particular risk is temporary staff. Thus you must credit reference and vet all staff as a matter of course
- If possible telephone all customers making new account applications – but obtain the customer's telephone number independently from the application form (as the one quoted could be false)
- Encourage customers to personally collect important documents rather than posting them out
- Train your staff to know about identity theft and how to identify it

LINKS

NCIS: The recent briefing note entitled "The Role of identity fraud in underpinning serious and organised crime" can be found at www.ncis.co.uk/briefing/270203.asp

FRAUD, CONCEPTUAL ART OR ADMINISTRATIVE TERRORISM?

In our experience one of the normal excuses given by fraudsters to explain their actions is that they were trying to show, in purely theoretical terms of course, that large security loopholes existed in the target of their attack. This concept has been taken a stage further by two French men who have (dependant on your point of view) either committed a large scale fraud or alternatively have merely constructed a valid conceptual art form that they have dubbed "administrative terrorism" (which on reflection may not be such a wise term to use in the current world situation).

Laurent and Benjamin formed an art collective in 2001 called Metastasis and began by displaying posters on the Paris ring road containing such quotes as "While you're stuck here, others are making love". The collective then took on a much larger, more cumbersome and inefficient target: French bureaucracy. They created 'virtual characters' which they then brought to life by applying for real documents in their names. In October 2001, Marc Duval (a fictional character presumably named after the 16th Century French artist) was issued with a legitimate French ID card by Montreuil town hall.

Spurred on by this success bank accounts, tax records and a company were set up in the names of non-existent people. Laurent told 'Le Monde' that "We had uncovered a real fault in the system...I honestly think that we could have carried on for years – even after getting a totally unjustified rebate of € 5 million paid into the bank account of a completely imaginary character called Mr. Chevalier".

Metastasis aimed to "shock individuals by forcing them to react" and claim that they tried to make these activities public "but no one wanted to know". Their exploits finally attracted attention when a retired man in the Val d'Oise department (who had the same name as one of the virtual characters that had been created) told the local tax authority that he did not think that the €3 million rebate that he had received was his.

The somewhat astonished police who arrested Laurent and Benjamin (no family names have been quoted) were told by them that they had tried to make their art work public by sending the authorities a registered letter explaining that "certain errors had been committed", but no one had taken any notice.

The reaction to these events have provoked widely different reactions: the pair's lawyer claims that they "exposed major administrative failings and performed a valuable service" whilst the central tax authority said that it will be pushing for the stiffest possible penalty.

MONEY LAUNDERING VIA PREMIUM RATE PHONE LINES

The Jersey Financial Services Commission in their February 'Enforcement Update' draws attention to money launderers using premium rate phone lines to wash dirty money. The normal use of facilities

involves the person or company that wishes to use a premium rate line signing up with a telephone line provider. When a caller then uses the premium rate line the telephone line provider bills the customer for using the line. These funds are then split between the telephone line provider and the subscriber (also known as the "content provider").

Showing once again that launderers are totally adept at using technology and business services for their own ends, they have corrupted this process to their advantage. The money laundering version has at least two variations as follows:

- The money launderer sets up as a content provider. He has a set of telephones that he uses to dial the premium rate numbers. He then pays the telephone bills he receives with dirty money, but then the telephone line provider pays the launderer his percentage of takings from the premium rate lines – in clean money
- An alternative, which has the same result is that the launderer has a network of people who agree to make calls to his premium rate number(s) and leave their telephones connected to them for long periods (such as overnight)

GLOBAL NEWS ROUNDUP

UNITED KINGDOM: At the beginning of February Ian Burns, a former professional footballer at Everton began a three year jail sentence for his role in a bogus investment scheme. Between 1995 and 1997 his firm, KB Securities, raised \$4.5 million by promising clients high returns, partially through repeat trades on a secret worldwide exchange. Somewhat unsurprisingly no such investment programme existed. An investigation by the Serious Fraud Office found that Burns and his business partner, Michael Kupfer had spent \$2.2 million on a life of luxury.

UNITED KINGDOM: In another case strangely similar to the one above, two men were jailed at the beginning of March for operating a 'high yield' investment scam that took about £2 million of investors' money. James Cadwell and David Curley received sentences of up to five years imprisonment. The investors were drawn from the UK, US and Austria and were told that their money would be put into "trading programmes" and given written undertakings that the funds were held in "tradeable securities or cash". There were no such programmes and the pair used the money for their own purposes.

ITALY: A conspiracy theory resurfaced again at the end of February, but this time it appears that it might not be so far fetched. A report delivered to Rome magistrates, concluded that all the available evidence pointed to the fact that the victim was murdered. Who was this victim? Roberto Calvi, the Vatican connected financier who was found hanging beneath Blackfriars Bridge in London during 1982.

SPAIN: Alberto Cortina and Alberto Alcocer, two of the most flamboyant figures of the Spanish business scene were jailed in mid March for three years and four months for defrauding investors in a Madrid property deal. 'The Albertos', as they are known, are cousins and co-chairman of Banco Zaragozano. The Spanish Supreme Court ruled that they had falsified documents and defrauded fellow investors in a property deal with the Kuwaiti Investment Office. The Albertos obtained a much higher price for themselves than for minority shareholders in the sale of land owned by their property group Urbanor to KIO. The Albertos have been ordered to repay €24 million to the other shareholders in Urbanor.

UNITED STATES: In a somewhat sickening turn of events, US citizens are receiving calls from various scam artists in connection with war homeland security. One example is where a call is received from a person claiming to be a representative of the US Government. The caller states that it is a requirement to purchase a survival kit, and the amount of purchase will be deducted from the checking account of the call's recipient. A US Better Business Bureau spokesman reinforced the obvious care needed to be taken by consumers by commenting that "No federal government agency would ask for your credit card, checking account number, social security number or any other personal information over the phone".

FROM NIGERIA: In an ingenious variation on 419 frauds, US officials have warned about a new type of scam utilizing Internet auction sites. In the new fraud, consumers selling goods on the Internet are approached by a potential buyer from Nigeria offering to buy an item at or above the asking price. In return the seller is asked to wire the balance of the inflated funds to a nominated bank account of the buyer. The buyer sends a cashier's check, which is counterfeit. However it is fairly normal practice for banks to make funds available before such a check actually clears – thus the seller wires the excess funds – only to find that the check that has been given to them is worthless.

NETHERLANDS: In yet another 419 scam variation, e-mails are being received from Hurry Securities, a Netherlands firm that congratulates the recipient on winning US\$6.5 million on the Dutch lottery. The catch? To claim the prize the lucky winner has to pay \$7,900 to cover costs of opening an account, handling, transfer, insurance and mail costs.

UNITED STATES: On March 24 the CEO of US Technologies, C. Gregory Earls was charged in a \$15 million fraud scheme that a prosecutor called “a naked theft of investors’ money”. Earls faces a federal grand jury’s 22 count indictment including multiple counts of securities, mail and wire fraud. Earls is alleged to have taken \$5.3 million from investors to launch an Internet company and then pocketed \$1.3 million for himself. Earlier charges allege that he misappropriated at least \$13.8 million from USV Partners, a company that invested in US Technologies. Authorities say that some of this money ended up in an educational trust for Earls’ children and his ex-wife and some of it was used to repay investors from other business ventures.

UNITED STATES: The US Treasury’s Financial Crimes Enforcement Network (FinCEN) has imposed a \$3 million penalty on Western Union for widespread currency transaction and suspicious activity reporting failures under the Bank Secrecy Act. Western Union have already been fined \$8 million by the New York State Banking Department for the same offences. A routine New York Banking Department examination discovered that the company had not filed almost 600 Currency Transaction Reports and 63 Suspicious Activity Reports during a two year period. Western Union blamed computer problems for these errors.

AUSTRALIA: In a widely publicised series of events, customers of the Commonwealth Bank were duped into revealing details of their accounts over the Internet. Customers were sent an e-mail urging them to follow a link shown in the message to “Re-activate their accounts” and make them more secure (!!). The link took the customer to a fraudulent website that resembled Commonwealth Bank’s genuine NetBank. Once there, the customer was fooled into revealing account details. Commonwealth Bank has stated that customers numbering in the “low hundreds” were taken in by this scam. Australian Police have already arrested one person in relation to this, with investigations continuing both in Australia and offshore.

RUSSIA: It has been estimated that 1.5 million stolen cars are being driven around Russia. High value prestigious marques make their way to the country after being stolen to order in Western Europe. To facilitate the trade, Customs officials are bribed and a new set of documents for the car are obtained from ‘helpful’ police officials. The cars are registered in the name of a dead person or someone who is homeless and then sold on. Oleg Yelnikov, from the Russian Ministry of Interior’s Organized Crime Directorate highlighted the problem when he was quoted in “The Observer” (UK): “From one side the former foreign owner has received his insurance payout and does not want the car back. We can’t punish the Russian buyer because the majority buy a car that seems registered legitimately to someone – be they homeless or fictitious. We can punish the road police – dozens were sacked in 1999 and 2000 – but after all of this, who is going to pay to take the car back to the owner?” The problem is particularly rife in Germany, where it is estimated that 30,000 cars each year are stolen. As ultimately insurance premiums go up as a direct result of this trade, one expert has commented that the ironic situation exists that German motorists are paying for criminals in Russia to drive better cars than them!

THE FINAL WORD

A fake police station in Sao Paulo, Brazil was doing brisk business collecting fictitious fines – even though it was only 100 yards from a genuine one. The fraudulent version was staffed by bogus officers who charged high fees to anybody who arrived to ask for help. The real police only realised when two men complained of being blackmailed.

In February Police in Buffalo Ridge, South Dakota acted swiftly on a terrorist alert. Motorists had raised the alarm when they saw a man of Middle Eastern appearance wearing a gas mask whilst driving a white van. The suspected terrorist was released when he told Police officers that he was delivering food and didn't like the smell of it.

A Russian man allegedly made hoax calls to the police telling them that there was a bomb in a public spa at Ulyanovsk. It just happened that on the day of the alert, it was women's bath day – and the would-be bomber hoped that the women would evacuate the building by running into the street naked. He was disappointed in more ways than one – the women got dressed before leaving the building and he now faces a jail sentence of up to three years for deliberately giving false information about an act of terrorism.

PROXIMAL CONSULTING SERVICE DIRECTORY

NEWSLETTER SUBSCRIPTIONS & PREVIOUS ISSUES

You can subscribe to this newsletter and download all previous issues at our website, www.proximalconsulting.com

KYC DUE DILIGENCE WARNING NEWSLETTER – Can you afford to be without this critical intelligence?

We also publish a monthly Know Your Customer Due Diligence Newsletter. The March edition contained warnings relating to over 200 individuals and/or companies currently known to be involved in fraud and money laundering. The annual subscription to this newsletter is £250, which includes a cumulative MS Excel spreadsheet that contains details of all warnings issued by us. You can get further details of this newsletter at: www.proximalconsulting.com

DUE DILIGENCE REPORTS

We conduct due diligence enquiries on individuals and companies on a worldwide basis. For full details of our fixed price services in this area please call us on +44 1672 516725

ASSET TRACING PROJECTS & OTHER INVESTIGATIONS

With our global network of associates and contacts we are able to provide a cost effective and proven solution to all your investigative problems – please call us for a confidential discussion on +44 1672 516725

PUBLICATIONS BY PETER LILLEY

Copies of Peter Lilley's two most recent books, "Dirty Dealing: the untold truth about global money laundering" & "Hacked, Attacked & Abused: Digital crime exposed" can be ordered online at www.kogan-page.co.uk

A new, fully updated edition of "Dirty Dealing" will be published in May 2003 – full details will appear in future newsletters and on our website

© PROXIMAL CONSULTING MMIII

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