PROXIMAL CONSULTING WHITE PAPER 9
THE FUTURE OF FRAUD ON THE INTERNET - RIGHT HERE RIGHT NOW

A 1997 survey by the US Computer Security Institute and the FBI's Computer Crime Squad found that 75% of 563 companies had financial losses of more than $1000 million from computer break-ins. Only 17% of those polled said that they would report the crimes to law enforcement authorities. Crimes by "outsiders" had increased to 47% of the total.

"I'm not so much concerned about the return *on* my principal as I am about the return *of* my principal" - Will Rogers

The future is what happens in a nanosecond's time: so in a very real way the future is right here, right now. Not that the future of fraud will be that different from the past: the brave new frontiers of the Internet, the former Soviet bloc and whatever else comes along simply present fresh opportunities to repackage tried and tested scams to victims (both individuals and organizations) who ought to have learnt better.

The Internet is a wonderful mechanism for criminals, because in cyberspace everyone is equal - if a webpage says that the company behind it is a well-regarded, long established concern who are you to doubt them? If they want money up front why should you question it? There are many enthusiastic Internet users who are only too willing to be convinced by the flashy websites detailing cybershopping, chain letters, pyramid schemes, work at home plans, phony investments and fake off shore banks (to name but a few frauds). These avid prospective customers would do as well to visit the Fraud Watch site first and dwell on its motto borrowed from P T Barnum: "There's a sucker born every minute." In actuality across the globe there are probably thousands, rather than one, born every minute.

The future both for providing information and acquiring customers is, we are told almost daily, somewhere in cyberspace where we join the 50 million people worldwide who have so far signed up for the Internet. This subject, and the closely overlapping topic of information warfare - crime and terrorism of the very near future will be waged by attacks on IT systems - is now very much a topic in itself, and it is only possible to scratch the surface here. It is a brave new world where all the lessons we have learnt in the old world have been forgotten....

No one knows the scale of Internet fraud - in May 1999 estimates for fraud in the UK caused by the Internet range from £400 million to £5 billion. Even more interestingly though: in the same month it was reported that an official at Visa International Inc in the States had commented that half of Visa's transactions from on-line sales are disputed or fully fledged frauds.

- Flashback to early 1997: In Hamburg, Germany the hacker group, The Chaos Computer Club, demonstrated on live TV the security loophole they discovered in Internet home banking software. They claimed that this could affect nine million people who use Quicken (a home and business accounts program) to check balances and suchlike on-line. The hackers demonstrated how they could take money from other people's accounts so that neither the bank nor the account holder was aware of the transaction until the next bank statement was issued.

- 1997: In London, a 19 year old schoolboy was fined £1200 for unauthorized access to secret US Air Force computer systems. Richard Pryce had previously been described to the US Senate armed services committee as "the number one threat to US security". He downloaded scores of secret files including the details of research and development of ballistic missiles. The Pentagon expected to find an Eastern European spy ring responsible for the 200 security breaches, not an A level student taking an obsessive academic interest in computers using a £750 home machine. In court the US military file security systems were described, with a large measure of understatement "as leaving something to be desired".

- Almost every US federal agency on the network has been penetrated including the Defense Department where hackers have entered systems which include researching ballistic weapons and submarine construction. Seven young men were arrested in Denmark for allegedly hacking into the US national weather service - without which US Air traffic control would be grounded throughout the country. Ironically these attacks appear to have been funded through over $1 million worth of credit card calls fraudulently charged to users in the US. One method used by the hackers was to persuade Americans over the phone to give their credit card numbers by posing as AT&T security officials.

There is a statistic somewhere which states that a human being has to make the same mistake seven times before he realizes that it is an error. To translate that into the business crime environment, why does anyone presume that the same old tricks won't work as well (if not better) in new media and delivery channels....and why does it take the "innocent" so long to learn this -

and the ethical companies so long to comprehend that however and wherever they operate there will always be an overlapping queue of people waiting to rip them off.

The following examples have just about everything - most pertinently all of the factors that we can predict will cause problems in the future (but as these events have already happened then the future must already be here now).

"As regulations get tougher in traditional offshore havens, criminals are finding a safe haven on the Internet and reaching a wider audience"
William Perez, FBI financial crimes expert (April 1998)

European Union Bank (EUB) was founded in 1994 by two émigré Russians. The rumour from the beginning was that it was used by the Russian mafia to launder money. The bank was incorporated in Antigua (which has 57 or so offshore banks registered there for its 60,000 inhabitants and is a constant cause of extreme concern for both regulators and law enforcers). Claiming to be the world's first offshore bank on the Internet, its main advertising was done, naturally, via its website - which included at various times:

- A one year $1 million certificate of deposit that paid interest of 9.91% - sometimes its interest rates were ten times that of its competitors
- "EUB provides clients with total privacy and….strict confidentiality…under Antiguan law no person shall disclose any information relating to the business affairs of a customer…except pursuant to an order of a court in Antigua. The court can only issue such an order in connection with an alleged criminal offence. There is no exchange of information treaty between Antigua and any other country."
- "The ultimate incentive to clients is an internationally attractive interest rate offered in the milieu of a tax free jurisdiction"

I'm sure you get the picture…and can predict the outcome. A bank nobody had heard off in an obscure offshore location? Too good to be true promised financial returns? In October 1996 the Bank of England drew attention to EUB's activities and warned that prospective depositors should carry out due diligence on it. Still the money poured in… until August 1997 when the bank was shut by Antiguan authorities after an investor had tried to unsuccessfully withdraw his investment of $128,000. Whilst it may or may not have been the first offshore bank to be established on the Internet, it certainly was the first failed fraudulent offshore bank there. There was no sign of the Bank's founders….or funds. Of course as it was an offshore private bank depositors went to it for discretion: thus it may be difficult to identify customers who will admit depositing money, never mind tracking down what funds were stolen. Press reports at the time commented on "wealthy investors" and "heavy losses".

Whilst European Union Bank may be the only false financial institution in cyberspace which has received publicity and failed very publicly, there are many more out there. Since January 1996 the US Office of the Comptroller of the Currency has issued over ten alerts about "banks" operating on the Internet. These warnings include the Excelsior Bank of Barbados and the First Lenape Nation Bank, operated by the Delaware Indian tribe of Andarko, Okla. The Freedom Star National Bank of Phoenix offered certificates of deposit with an 18% yield through its web site until regulators pressurized its president to close it down. Netware International Bank based in Mooresville, NC took in over $1.2 million in deposits - at least that was what the FBI seized together with the "Bank's" records.

Internet "Banks" can not only defraud the innocent but also be a front for organized crime - so who does have jurisdiction and regulatory powers in Cyberspace? The awful truth is that a "virtual" fraudulent bank (or any other type of virtual company which defrauds gullible customers) if done with style and a modicum of intelligence is virtually untraceable and unprosecutable - and the funds it has taken in are unrecoverable.

A ONCE IN A LIFETIME CHANCE TO CASH IN ON THE MILLENNIUM BUG. BY THE YEAR 2000 YOU COULD TRIPLE YOUR MONEY.

SO WHO IS MBI?

MBI was founded in 1997 by 3 Swiss business leaders….the company was set up for the sole purpose of providing blue chip companies and governments with insurance against Millennium Bug problems. After its huge success in Europe and the United States, MBI is coming to Australia. MBI is establishing offices in Canberra, Sydney and Melbourne by the end of May 1999.

GUARANTEED PROFITS!

It is confidently expected that investors will triple their money between the time of the investment and September 30, 2000 after which time the insurance policies become null and void.

Yes, you should expect to make a return of 200% on your investment in just over 15 months…..

HOW DOES THIS INVESTMENT WORK?

The explanation is simple. Because of the lack of competition in this category, and our unique expertise, MBI & its investors can achieve extra ordinary levels of profit….

SO HOW EXACTLY DOES IT WORK?

It all sounds too easy.

MBI has a group of IT experts with leading edge knowledge of the Millennium Bug. With detailed analysis of computer systems and operations we are able to classify corporations and government departments into 5 separate risk categories. We can then target the corporations and departments that fall into the two lowest risk categories. We make approaches to them at the highest level offering our underwriting services. These insurance premiums are heavily loaded beyond normal underwriting criteria because of lack of competition in this market.

You can receive GUARANTEED RETURNS for your INVESTMENT OUTLAY

More than 10,000 potential investors visited this website. Eleven people complained that this website set up on 1 April 1999 was a fraud. 1212 potential investors asked for more information. 233 people pledged investments totalling in excess of Australian $4million.

In May 1999 the Australian Securities and Investments Commission put their hands up and admitted it had all been an elaborate April Fools Day joke to highlight the danger of fraudulent investment scams on the Internet. ASIC chairman Alan Cameron hit the nail on the head when he commented that "investors should be wary of fraud and not believe that the Internet offers some sense of instant authority."

Ironically, also in April 1999, the United States Securities and Exchange Commission was granted an emergency restraining order against "Prince" Lazarus Long (also known by the more prosaic name of Howard Turney) who was offering what the SEC claimed to be bogus bonds on his New Utopia website - which at the time of the complaint by the SEC had received over 100,000 hits. Believe it or not New Utopia -whose website is still there at the time of writing: I know because I've just been on it- is a country which will appear out of the Caribbean on giant concrete platforms built on a land mass 115 miles west of the Caymans Islands. I really wanted to believe this (?) but the clincher was the information on the Prince's partner, Princess Maureen!! The serious side to this is that the website offered:

- Unregistered 5 year New Utopian government bonds promising a 9.5% return -which were promoted by e-mail by the Prince
- Up to a 200% return on New Utopian currency investments
- The opportunity for investors to become charter citizens of the new country

The moral of the story? If the Australian Securities and Investments Commission can gather US $2.65 million worth of investment pledges on a deliberate fake site then it appears that gullible investors across the globe will be taken in by anything....Why? Don't ask me, I really haven't got a clue. One would have thought that anyone wishing to invest their own money would take care - but obviously not. People, almost unbelievably want to be ripped off - www.fraudexplosion.com is right here, right now.

You need more proof? Back to the SEC. In May 1999 they launched 14 enforcement actions against 26 companies and individuals who were alleged to have used the Internet to defraud potential and actual investors (thus it must be pointed out that at the time of writing all of these actions are still pending). Whilst this is laudable I have this nagging suspicion that we've returned to the very tip of the iceberg scenario. What strikes me is that all the same maxims about preventing fraud apply. Moreover it is surely not the medium but the message: by that I mean that these cases are not Internet fraud per se, just that the Internet has become a marvellous worldwide delivery channel for tried and trusty rip offs. All you web surfers are just waiting to be taken in by the likes of:

- New Yorker David Abramson who offered securities in a gold venture on two websites. On one of these websites he claimed that investors would receive gold in quantities equivalent to returns ranging from 800 to 2600% annually for ten years. Using the style "Brightstar Gold" Abramson falsely, the SEC allege, claimed that this entity had a ten year contract for the supply of a "gold rich" magnetite concentrate. Additionally Brightstar would use a proprietary processing technology that enabled it to deliver gold to its investors "at a fraction of its market value".

  Total invested by the public: $50,000 plus.

- Abacus International Holding is owned by Arthur Agustin, and from July 1998 its web site sold "prime bank" securities, guaranteeing modest returns of 80% per month and higher! The Abacus website claimed that it was an international company (Agustin operated it from his home). The SEC allege that in fact much of this website was compiled from materials found on other websites.

  Total invested: $180,000 from one investor who was induced to send a further $80,000 to a third party

- And yet more of the same from a Massachusetts business consultant, Richard J Briden and his two corporations Empowerment Funding Group and Infopro Group. The SEC allege that through the companies two websites prime bank trading programs were touted which required a $1 million minimum investment. Investors were promised as much as 100% return per week - with no funds leaving the investors bank account. The SEC's complaint goes on to allege that Briden convinced at least three investors to provide him with proof of their $1 million investment and signed powers of attorney giving him the mandate to commit funds to the "Million Dollar Programs". It is also alleged that seven further investors were convinced to invest $295,000 in another "risk free" prime bank trading program. These funds were transferred to a Guernsey bank account in the name of Mutual Assets Limited. None of the return promised to these investors has materialized. The SEC allege in their complaint that Briden has explained that the returns have not been paid because of: bank holidays, sickness of some of the traders, bank mix ups and various other excuses.

- HDG Investment Corporation (a BVI company) and Paul J Edwards (a Canadian living in Prague) have been charged with fraudulently raising over $300,000 from investors in a prime bank scheme which according to the commission does not exist. Investors were promised a 20 to 1 return on their investment in thirty days!

- Among other alleged frauds in the SEC's sweep are another "non-risk" prime bank program promising a $3,000,000 return in 10 months on an investment of $35,000; a scheme which promised returns of 10% to 400% per month without risk by investing in "secret" foreign trading markets; a software start-up company which projected investment returns of 500% to 2000% in two years which gathered $50,000 worth of investments; a foreign currency trading scheme which could have lost investors as much as $2 million; yet more prime bank guarantees; it goes on.

I could also go on and on: but I'd rather quit whilst I'm ahead and more importantly before I actually start believing that surely one of these scams must be true. Defend yourself against the explosion: the final advice I can offer is what used to be said at the end of the prelude to each episode of "Hill Street Blues": Be careful out there.....(wherever there is).

November 2003 – Adapted from "Hacked, Attacked & Abused: Digital Crime Exposed" by Peter Lilley (Kogan Page, 2002)

Proximal Consulting

Email: enq@proximalconsulting.com

Telephone: +44 (0) 1672 516725

Offices:

Poughcombe Barns
Ogbourne St Andrew
Wiltshire
SN8 1SE
UK

Rue Du Rhone 14
1204-Genève
Switzerland

Proximal Consulting have unrivalled experience in providing KYC enhanced due diligence background reports on individuals and companies on a global basis. We also offer a complementary range of services including AML training, country risk reports and bespoke investigations.

Our enhanced due diligence reports are tailor-made to our clients' specifications. They are totally different from the usual database-led reports that often fail to meet enhanced due diligence requirements. Our reports present clear, accurate and confidential findings which enable our clients to make informed business decisions and to fulfil their AML obligations.

We work with a variety of global clients including regulatory agencies, law firms, individual companies, private banks, trust companies and other firms in the financial sector.
