

# Internet Fraud

The view expressed in this paper are the views of the authors and do not necessarily reflect the views or policies of the Asian Development Bank (ADB), or its Board of Directors or the governments they represent. ADB makes no representation concerning and does not guarantee the source, originality, accuracy, completeness or reliability of any statement, information, data, finding, interpretation, advice, opinion, or view presented.

**APEC Financial Regulators Training Initiative  
Regional Training Program**

**INVESTIGATION, ENFORCEMENT and PROSECUTION**

**26 November – 30 November 2001  
Manila**

# Internet Fraud

Presented by:

Keith Inman

Director Electronic Enforcement

Australian Securities & Investments Commission

Email: [keith.inman@asic.gov.au](mailto:keith.inman@asic.gov.au)

Web site: <http://www.asic.gov.au>

The views expressed in this paper are the views of the authors and do not necessarily reflect the views or policies of the Asian Development Bank (ADB), or its Board of Directors or the governments they represent. ADB makes no representation concerning and does not guarantee the source, originality, accuracy, completeness or reliability of any statement, information, data, finding, interpretation, advice, opinion, or view presented.

## Investigation Particular Cases: Internet Fraud

### Case Study A

The following scenario is taken from a recent ASIC case and relates to illegal investment advice supplied over the Internet.

To prove such a case involving an individual suspect, in the days of the 'old economy', you would need to interview witnesses who had received the advice and take possession of admissible evidence. Be that as oral evidence or in the form of correspondence.

In so doing it would be necessary to prove where the correspondence came from and handwriting, signatures or fingerprints helped solve that particular problem. A search warrant might even turn up photocopies or examples of similar letters to other victims. Generally, there would not be too many people who had to be interviewed or, a great deal of evidence needed to prove the elements of the offence.

In the new economy, many of those sources of evidence don't exist anymore and only some of them have been replaced by their electronic equivalents. Furthermore, much of the evidence is perishable, dissolving over time. As a result, all investigations will involve a degree of added complexity.

In the new economy, the perpetrator doesn't need paper correspondence; he does it via a bulletin board on the Internet. He doesn't own the web site (which we will call MakeMoneyFast.com.au) he just visits to post his messages and respond to those people who answer him. He's not a financial wizard as such. He doesn't even work in the financial sector. In fact he is a graphics artist for a marketing firm.

There is no cost or registration process involved if you want to view the messages on the bulletin board at MakeMoneyFast.com.au. The owners of the site make their money from advertisements. In order for a person to post a message to the forum, however, they must first become a registered member. So this is what our perpetrator did, he registered the on-line identity *Hot Trader* under the false name Michael Mouse.

*Hot Trader* made two postings giving investment advice to people via the site. So lets have a look at what we had to collect to prove this matter:

1. There are a number of basic searches that start the process off. Domain names must be registered though one of a number of organizations. One such organization is the Australian Network Information Centre ("**AUNIC**").

AUNIC has an Internet based register of domain names that records the name and details of the registered owner of a '.au' domain name. A WHOIS search of the AUNIC registry tells us who has registered the domain name MakeMoneyFast.com. **Company A**. So we have collected our first piece of evidence.

2. Each computer connected to the Internet must have a unique Internet Protocol number (IP), a sequence of 4 numbers. The IP address allows that computer to be identified and for data to be sent between that computer and other computers that are connected to the Internet.

When compared with the ordinary postal system, the IP address is like the delivery and return address written on an envelope. Generally speaking, by tracing an IP address it is possible to identify a particular computer responsible for the transmission of data over the Internet.

But we rarely see the IP number up front. Because it is not easy to remember a sequence of 4 numbers we use Domain names like MakeMoneyFast.com.au.

3. The 'Domain Name System' ("**DNS**") is the way that domain names are translated into IP addresses. There is no central register of domain names and their corresponding IP addresses. Instead, a complex system of DNS servers 'map' domain names to the correct IP address.

The DNS system can be searched to identify the IP address that corresponds with a particular domain name. This gives us the **IP address 'Z'**.

IP addresses are allocated by 3 regional Network Information Centres. The Asia Pacific Network Information Centre ("**APNIC**") allocates IP addresses in the Asia Pacific region. APNIC maintains a database of all IP addresses it has allocated.

A check for IP Z reveals it is owned by **Company 'B'**.

*(Our investigation has not gone very far and yet we have already been dealing with 4 organizations.)*

4. Inquiries with the two companies reveal that **Company 'B'** hosts the Bulletin Board site for **Company 'A'**. This means that the data that makes up a website is ordinarily located or housed in a computer server owned by a third party that offers web hosting services.

The web host will provide computer servers, technical support and the

access point to a communications network that will allow a website to exist on the Internet. Therefore a common way of operating a website is to contract with a web host for it to "host" your website.

5. We need copies of the two posting that constitute the advice. Company 'B' supplies them to us in response to compulsory notices. Each posting includes a header recording the name of the poster (in this case Hot Trader), the date and time it was posted, and the Internet Protocol number of the source of the posting. We know from Company B that the name Hot Trader is registered to Michael Mouse. So that doesn't get us anywhere. But we have two IP numbers, X and Y, to work with. From Company B (the site host) we obtain the Web Server log file record for the relevant dates and times.

A web server program processes requests for web pages and delivers the relevant files to the requesting computer. A web server log file records the web server's activities. This confirms that the header information is correct.

6. The next step was to conduct more APNIC checks to identify the registrant of the IP 'X' number. It turned out to be an Internet Service Provider: **ISP 1**. Using compulsory notices, we required the ISP to provide us the Proxy Server logs for the relevant date and times.

A Proxy Server is used as a 'gateway' between an internal computer network and the Internet to ensure security and administrative control. The Proxy Server log file extract confirmed that IP address 'X' made a "POST" to the Bulletin Board website at the relevant date and time.

The next stage was to require the ISP to provide its IDX Remote Authentication Dial-in User Service ("**radius**") log record for IP address X. This basically recorded which ISP customer was logged onto the Internet using IP X at the relevant date and times.

We then obtained the application form for the Internet services and in this case the person paid using a credit card. So we had a suspect. It isn't always that easy. Often people will purchase ISP services by paying cash over the counter and receiving a CD that provides the necessary connection details.

7. OK, so we have found a suspect for posting number 1. Lets now look at posting number 2. An APNIC check of IP address Y indicated that the IP was allocated to a private company in Adelaide. **Company C**.

A compulsory notice was again used to obtain the company's firewall logs for the relevant times. A 'firewall' is a software program or a

hardware device used to prevent outsider access to an internal network and also to control which outside resources the internal users have access to.

A firewall log file can record the IP address of the internal computer accessing the Internet via the firewall. The firewall logs confirmed that their IP number had accessed the Bulletin Board site and had been used to post text to the site.

Unfortunately for us, the company did not have the relevant logs turned on to capture which user was accessing IP number Y at that particular moment. This was an oversight on behalf of their system administrators and a real compromise of their internal security framework.

Our inquiries with the company, however, revealed that the suspect was an employee. Using search warrants, we obtained a forensic examination of the suspect's office PC and within the Internet Cache of the PC located copies of the offending posts.

## **Case Study B**

This scenario deals market manipulation case involving the Internet. The perpetrators buy a quantity of cheap shares then entice the investing public to buy the same shares on the basis of false and misleading statements made on the Internet.

As more people buy the shares the price increases and the perpetrators sell their holdings for a considerable profit. When investors realize what has happened the share price collapses leaving most of them holding shares worth considerably less than they paid.

The Australian perpetrators start on the weekend when the stock markets are closed. Information containing false and misleading statements about a particular U.S. company are posted on the Internet to finance related bulletin boards in the U.S.

Over the next two days millions of unsolicited emails (SPAM) are sent to recipients in both the US and Australia alerting them to this new information. When the stock markets open on Monday morning there is a rush to buy the shares and the price claims quickly. By 12pm on Monday it is exposed as a scam, the stock is suspended from trading, the company releases a press release and the share price collapses.

In an effort to hide their tracks, the perpetrators;

- Buy and then sell their shares through an on-line stockbroker in a foreign country.
- They opened accounts with more than one Internet Service Provider (ISP) in different States in Australia.
- They buy the ISP services using cash over a counter at a retail shop by purchasing several pre-paid compact discs.
- When dialing into the ISPs they use fictitious names and multiple telephone lines.
- Furthermore, in an attempt to confuse the electronic trail, they relay their SPAM through computers owned by innocent third parties around Australia.

One of the most important lessons to learn from these case studies is that if parties to electronic transactions do not have their system logs turned on and being archived, they won't even know they have become a victim – never mind having sufficient records to support a civil restitution process or a criminal prosecution.