



Financial Supervision Commission

P.O. Box 58, Finch Hill House, Bucks Road, Douglas, Isle of Man, IM99 IDT

IDENTITY THEFT

Common sense advice for Financial Institutions and Consumers

The Financial Supervision Commission ("FSC") have recently issued a number of Public Warnings on the subject of Identity Theft. These Warnings may be found in the Public Warnings area of the Commission website at www.fsc.gov.im

The recent case, widely reported in the press, of Mr Derek Bond, a 72-year-old British Citizen arrested in South Africa in a case of mistaken identity which appears to have resulted from having his identity stolen some 14 years previously, has brought this subject into the public eye.

The Commission offers the following information in order to assist both Institutions and Consumers from becoming the targets of this problem, which is, apparently, becoming increasingly prevalent.

Advice for Institutions

These common sense suggestions are likely to already be in place. Several potential Identity Theft cases have come to light recently on the Island, however, in all of the cases that the Commission has been advised of, institutions have played an important role in alerting the victims. The suggestions are intended to assist you in considering whether there may be weaknesses in your systems capable of abuse.

- Your routine anti money laundering checks also play an important role in discouraging identity theft. Be aware of this when reviewing the information provided. Be especially cautious where new customers claim to have recently moved address.
- Where customers contact you with a change of address consider steps to verify that the information has genuinely originated from the customer. Can you contact them at a work number already on file? Consider sending out confirmation of the change of address to both the new address and the old one.
- Be particularly suspicious if a customer orders a new credit card or cheque book at the same time as notifying a change of address.
- Don't give sensitive information out over the telephone unless the caller knows a password or can answer a question that an impostor shouldn't be able to know. If you don't have a specific procedure set up with the customer, this could take the form of a simple question about an earlier occurrence on file, for example a previous job or address or the date of becoming a customer. This is likely to be well known to the genuine customer but much harder for an impostor to obtain.
- Some victims of identity theft will put a "fraud alert" on their credit records asking that a confirming call be made whenever someone tries to open an account in that person's name. If such a situation arises please ensure that you make the call.

- There are some indications that recent attempts at identity fraud have originated in the interception of mail in overseas locations. Give due consideration to the appearance of correspondence. Will it be easily identifiable as containing potentially sensitive financial information; for instance, does it have the name of your institution on the outside or on the frank mark? Can it be easily opened and resealed without the genuine recipient being aware that this has taken place? It is common to show simply a postcode return address on the outside of the envelope. If this is the case can you be identified from it, for example does it appear on your website? If it does, will a routine web search on the postcode lead a potential scammer straight to it?
- If you are an Isle of Man institution and suspect that one of your customers is being targeted or that your customers may be being systematically targeted contact the Financial Crime Unit of the Isle of Man Constabulary at the very earliest moment by writing to:

The Officer in Charge
 Isle of Man Constabulary
 Financial Crime Unit
 PO Box 51
 Douglas
 Isle of Man
 IM99 2TD

Or by telephoning:

686000

Advice for Consumers

The Isle of Man Constabulary, Financial Crime Unit advise the following:

What is Identity Theft and Identity Fraud?

Identity Theft is, quite simply, the misappropriation of the identity of another person, without their knowledge or consent. Another name for this is impersonation fraud. The name and other personal details of the victim are used to obtain goods and services in the victim's name. Examples of the kinds of information that can be used may include date of birth, current address or previous address – the kind of information which is used to help establish identity in an application for all manner of services. Much of this information may be freely available in the public domain.

Identity Fraud is the use of the stolen identity in criminal activity, for instance, by obtaining goods or services by deception. Generally (but not exclusively) this involves the use of stolen or forged or fraudulently obtained identity documents such as a passport or driving licence. The press reports suggest that this is what happened in the case of Mr Bond.

Is it a serious problem?

For the victims it most certainly is. Often it will affect their credit rating and therefore, their ability to obtain finance, insurance, even a mortgage may, at least temporarily, be compromised. The problems which arise as a result can be very difficult to sort out. In the case of Mr Bond they resulted in an innocent man spending a several weeks in prison.

Recently released figures suggest that in 2002 alone, over 32,000 United Kingdom citizens were the victims of this type of fraud. It has been suggested that this is the most rapidly increasing type of fraud ever seen in that country. There is no reason to believe that the Isle of Man is immune to this.

Do you know whether you are a victim of Identity Theft?

It is important to remember that anyone can potentially become a victim of identity theft. It is fair to say that the better your credit rating and financial standing, the more likely you are to be targeted as a victim. You should be aware of the warning signs to look out for. The following list is not exhaustive but may provide some food for thought:

- Have your regular bank or credit card statements failed to arrive? Have you become aware that any of your mail has gone missing?
- Have you been contacted by a debt collection agency about goods that you have never ordered or in respect of an account that you have never opened?
- Are there charges on your credit card statement for items that you haven't purchased or ordered?
- Have you received a letter or telephone call advising you that have been denied or approved credit for accounts that you know nothing about?

How can you help to prevent yourself becoming a victim of Identity Theft?

- Never, ever, provide any credit card, bank or other confidential information to anyone by telephone, especially if they call you UNLESS you can positively verify that the caller is genuine.
- Consider ordering your credit file report once a year from one of the major credit reference agencies. Study the report for any unauthorised activity. If there is any suspicious information in the report question the account or make enquiries to enable you to get to the bottom of it. Most credit reference agencies should be able to offer help and advice if this situation arises.
- Do not carry your extra credit cards, utility bills, your passport, your birth certificate or other Identity Documents except when necessary.
- Always retain your credit card receipts, and securely destroy them before disposal.
- Never leave your wallet, purse or any identity documents unattended, or in open view in your car.
- Always reconcile your bank statements and credit card statements as soon as possible after receiving them. Notify the card issuer or your bank if there are any purchases that you did not make.
- If you make an application for credit or insurance by telephone or in a public place, for instance within a shop, be careful that you are not overheard by others. They may use the information in an identity fraud. If you end up with any waste paper keep hold of it and securely destroy it when you get home.
- Memorise your passwords and personal identification numbers (PINs) so that you do not have to write them down. When you are using cash machines be aware of your surroundings to make sure that nobody can see you input your PIN.
- Keep a list, IN A SECURE PLACE, of all of your credit card accounts and bank accounts. This will allow you to quickly inform all of the issuers about missing or stolen cards. On the list include details of account numbers and telephone numbers of customer service or fraud departments. Consider registering with a card protection company which will do this for you

should the need arise. Your bank may be able to recommend a reputable card protection company.

- Be wary of so called "credit repair" organisations. If you have genuine problems, your creditors themselves are the first ones that you should contact. Your local Citizens Advice Bureau can help you.
- If you move house, make sure that you put a mail redirection in place for at least the first year afterwards.
- Consider ordering your credit file report once a year from one of the major credit reference agencies. Study the report for any unauthorised activity. If there is any suspicious information in the report question the account or make enquiries to enable you to get to the bottom of it. Most credit reference agencies should be able to offer help and advice if this situation arises.
- Don't throw away credit offers without tearing them into small pieces or shredding them. These offers will often contain information which may be enough for an identity fraud. The same applies to other sensitive information such as, credit card receipts, bank statements, telephone bills and utility bills.

What do you need to do if you believe that you may be the victim of identity theft?

- Do not ignore it. It is not going to go away of its own accord, and the longer you leave it, the harder it will be to solve.
- Immediately contact everyone involved. Keep a record of all of your actions, details of who you spoke to and copies of all correspondence.
- Report the incident to the police, especially if it involves the theft of identity documents.
- If you lose a passport, driving licence or other identity document report it to the relevant authorities. Detail the circumstances of the loss.
- Report stolen cheques or credit cards to the issuers immediately. If you contact them by telephone follow this up with written notification. Make sure that you get new cards, account numbers and PINs. Don't continue to use a compromised PIN.
- If you suspect that mail theft has taken place or that a mail redirection has been fraudulently set up on your address contact the Post Office. They will be able to help you.
- If you close a bank account destroy all unused cheques and any cards immediately. Destroy expired cards.

Is anything being done to tackle the problem of Identity Theft?

Financial institutions go to great lengths to establish the identity of their customers. They are obliged to do this under Money Laundering Regulations. They are required to "know their customer" and to verify both name and address.

When opening an account proof of name and address is required and institutions also carry out independent checks using, for instance, electoral rolls, telephone directories and credit reference agencies. It is common for them to ask to see photographic identity documents together with a broad selection of other documentation such as recent utility bills, rates bills and the like. The broader the range of documentation they require the harder it is for unscrupulous persons to pass themselves off as you.

FSC Ref: News/JPM/05/2003