



Chartered Accountants' Hall
PO Box 433
Moorgate Place
London
EC2P 2BJ

Tel 020 7920 8721

Fax 020 7920 8545

Email info@fraudadvisorypanel.org

www.fraudadvisorypanel.org

26 May 2006

Mr Nigel Evans MP
Chair
All Party Parliamentary Group on Identity Fraud
House of Commons
London
SW1A 0AA

BY EMAIL: inquiry@idfraud.org.uk

Dear Mr Evans

Response and Comments on the Immediate Steps the Government Could Take to Combat Identity Fraud

The Fraud Advisory Panel ("the Panel") welcomes the opportunity to provide comment on the steps that Government could take to combat identity fraud.

The Panel response proposes three changes to legislation in order to combat identity fraud. The first two proposals relate to proposed amendments to the Identity Cards Act 2006, whilst the third proposal relates to the Data Protection Act 1988.

First Proposal

One of the unlawful ways used by identity thieves to infiltrate a victim's computer without consent is to use software, colloquially known as spyware. This enables the fraudster to covertly monitor and obtain details of all activities which the user undertakes online whether it be shopping routines, banking information, travel plans, online tax information and so on. This information is collated and sent back to the fraudster so that he may use it to apply for credit or a false identification document. In this way organised criminal gangs across the world can access databases of personal information without leaving their computers.

The Identity Cards Act 2006 provides:

"25(3) It is an offence for a person with the requisite intention to make, or to have in his possession or under his control:-

- (a) any apparatus which, to his knowledge, is or has been specially designed or adapted for the making of false identity documents; or
- (b) any article or material which, to his knowledge, is or has been specially designed or adapted to be used in the making of false identity documents.”

However, this offence does not restrict fraudsters accumulating information through the use of spyware, key loggers designed to steal information and the like.

Therefore the Panel proposes after Section 25(3)(b) to insert:-

- “(c) any apparatus which may be used to collect or otherwise receive registerable personal details of another, without that person’s consent.”

This amendment would then restrict the possession by fraudsters of, not only the machinery needed to produce fake identity documents, but in conjunction with the proposed revision to S.25(1), spyware used to accumulate stolen information.

This amendment still requires the fraudster to possess the requisite intention, meaning that legitimate uses for such software would vitiate the offence. Spyware is often used validly by marketing companies who develop the information gained from them to correctly gauge the potential market. This is usually accomplished with the consent of the computer owner just as key logging software is used by most computer engineers to assist employees who have lost or forgotten their login details or passwords.

Second Proposal

Given that the offences under S.25 Identity Cards Act 2006 are committed by reference to false identity documents, the definition of in S.26 is of vital importance.

S.26 provides:

In section 25 "identity document" means any document that is, or purports to be:-

- (a) an ID card;
- (b) a designated document;
- (c) an immigration document;
- (d) a United Kingdom passport (within the meaning of the Immigration Act 1971 (c. 77));
- (e) a passport issued by or on behalf of the authorities of a country or territory outside the United Kingdom or by or on behalf of an international organisation;
- (f) a document that can be used (in some or all circumstances) instead of a passport;
- (g) a UK driving licence; or
- (h) a driving licence issued by or on behalf of the authorities of a country or territory outside the United Kingdom.”

Section 4 and Section 26(4) Identity Cards Act 2006 empowers the Secretary of State to designate the description of documents falling under Section 26(1)(b).

However, the definition of what constitutes an identity document, does not effectively identify other forms of information collation and storage that are also necessary to protect the identity of the individual from theft.

The problem which exists is that even though being in possession of a false identification document is an offence, this definition does not extend to being in possession of the information which may be used to replicate a victim's identity.

The definition does not take account of the fact a person can be identified by means of either a single document such as a utility bill or a collection of information such as a database or Spyware report.

Therefore the Panel suggests that it may be more beneficial if one simply offers a wide definition of what a document is and to evaluate its applicability to unlawful acquisition of personal information on a case by case basis. This could be achieved by inserting after S.26(1)(h):-

“Any collection of registerable personal information of another, which has been collated without the permission of that person.”

Third Proposal

Recent large scale losses of personal data by companies, businesses and government departments over the last twelve months, including credit card details, employee details and national databases have exposed limitations in the protection afforded by the Data Protection Act 1988.

In response to this problem, the Information Commissioner recently stated that a report will be tabled before Parliament in the coming months which will request the creation of a custodial sentencing regime for data thieves who contravene the Act.¹ This is to be welcomed.

However, this still leaves the problem caused by data loss disclosure.

At the moment, the Data Protection Act 1988 does not place an obligation on those responsible for data to inform victims of data breaches or that their identities may have been compromised by a loss of data. This is a surprising omission as the fact that an individual's personal information has been lost to potential criminals is one of the matters that it was designed to prevent.

The matter is now being addressed in the United States where the States of Wisconsin and California require notification of loss to be given. The Panel suggests that the All-Party Parliamentary Committee may wish to consider the benefits of introducing similar legislation in the United Kingdom.

Under Senate Bill 164 (2005), Wisconsin businesses are now legally obliged to inform customers when their personal information has been stolen. This not only places a burden of accountability upon data holders to actively protect information, but also to keep tighter reins on data flow. Companies are required by the Bill (SB164) to alert their customers through

¹ www.vnunet.com, 15.05.2006

regular vehicles of communication about any security breach which may affect the information held by them.

Furthermore, affected individuals may still bring civil compensation claims against the data holder even if notification has taken place.

This legislation encourages data storers to take all reasonable steps to guard information in relation to their customers.

It may be that the data holder should be given discretion as to when notification should be given if immediate disclosure would hinder or obstruct the proper conduct of an investigation into the breach by the police or where the data holder is pursuing civil remedies.

The wording of the Wisconsin and Californian legislation is set out below.

Section 2 (a-b) of the California Senate Bill 1386 (2002), which was the precursor to the Wisconsin Senate Bill reads as follows:

- “SEC. 2. (a) Any agency that owns or licences computerised data that includes personal information shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorised person. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision (c), or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.
- (b) Any agency that maintains computerised data that includes personal information that the agency does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorised person.
- (c) The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification required by this section shall be made after the law enforcement agency determines that it will not compromise the investigation.”

The Wisconsin Senate Bill 164 (2005), takes a slightly simplified legislative style, and reads as follows:

- “SEC.2. (a) If any entity whose principal place of business is located in this state or an entity that stores personal information in this state knows that personal information in the entity’s possession has been obtained by a person whom the entity has not authorised to obtain the personal information, the entity shall make reasonable efforts to notify each individual who is the subject of the personal information. The notice shall indicate that the entity knows of the unauthorised use of personal information pertaining to the individual.

(b) If an entity whose principal place of business is not located in this state knows that personal information pertaining to a resident of this state has been obtained by a person whom the entity has not authorised to obtain the personal information, the entity shall make reasonable efforts to notify each resident of this state who is the subject of the personal information. The notice shall indicate that the entity knows of the unauthorised use of personal information pertaining to the individual.”

Yours faithfully

Steven Philippsohn
Trustee Director, Fraud Advisory Panel
Chairman, Fraud Advisory Panel Cybercrime Working Group