

Comments on Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice

23

From Mary P. Kirwan

355 St Clair Avenue west, Toronto, Ont. M5P 1N5, Canada

Security & Risk Consultant

(416) 838 4080

mkirwan@eol.ca

General Comments

In a recent survey conducted by the US Federal Trade Commission (FTC), the extent of the problem of identity theft was laid bare for the first time. It revealed that 27.3 million Americans had been victims of identity theft in the last five years, with 9.9 million alone in the past year.

These staggering numbers dwarfed all previous estimations of the problem, and caught even seasoned observers by surprise.

The cost to business, especially the financial services sector, appears to be enormous. The FTC survey estimated the damage to be in the region of US\$48 billion. The credit card companies have been criticized for not doing more to prevent identity thefts. Retailers have been particularly vocal about their concerns because they suffer as a result of 'charge backs from the card issuers in 'card not present' transactions, such as Internet and telephone transactions.

Many small retailers are unable to provide credit facilities to customers due to their exposure to various types of Internet fraud, as they are ill equipped to cope with the increasingly sophisticated nature of the crime.

Consumers are also paying dearly. They are often forced to mop up the problem themselves. According to the FTC survey, victims bear out of pocket expenses of approximately US\$5 billion to clear up credit histories and good names, and put their lives back together again. Frequently, victims are pursued by debt collectors and institutions that care little about the true identity of the individuals responsible for running up myriad unauthorized charges. Many victims have had their credit ratings and lives destroyed.

In the FTC survey, most of the victims (76 per cent) indicated that existing credit card accounts had been misused, and more than half of the victims (52 per cent) spotted the problem themselves. Only 26 per cent were notified by the banks or credit card companies, and an unfortunate eight per cent only found out when they had credit applications turned down.

Many victims do not find out that their sensitive data has been compromised until well after the fact. As a result, their ability to take steps to protect themselves against the consequences of the crime has been severely compromised. The window of opportunity for the thieves to use the stolen information is often tight, and time is of the essence if victims are to protect themselves. They can do little if they do not know the crime has occurred.

There may be a trend emerging for regulators to mandate reporting of security breaches in situations where identity theft is foreseeable. For example, SB 1386 in California mandates reporting to customers in defined circumstances, where they are at risk as a result of a security breach, unless the data is encrypted.

Statutes such as these are controversial, as companies, regardless of sector, or indeed size, have proven to be extremely reluctant to report security breaches to those affected, usually the actual data owner, for fear of negative publicity and market sentiment, and loss of customer confidence. Companies' reluctance to report security breaches results in a lack of reliable data to reflect the extent of the security problem. This in turn feeds perceptions in many circles that the problem is over hyped by the vendors (selling security products mainly through so-called FUD (fear, uncertainty and doubt) marketing).

However, there is a growing realization globally that the risk is escalating, and that it has the potential to negatively impact consumer confidence, at a time when consumers are driving growth in many sectors, and without whom the economy would be moribund.

Specifics:

I am doubtful as to whether reference to **'substantial harm or inconvenience to the customer'** is sufficiently precise terminology to be workable for all concerned. Does it mean 'substantial harm' or 'substantial inconvenience' or mere 'inconvenience' alone? What is meant by 'inconvenience'? This is a most subjective term. I believe this definition needs work - even 'harm' on its own would be better. Or the legal term 'loss or damage', which is at least well defined in case law.

And what is 'substantial'? If the concern is the potential for identity theft, the customer may be forced at a minimum to cancel accounts, scour statements and charges, but in hard cases, may be forced to fight off debt collectors, law enforcement (when falsely arrested as result of thief committing crimes in his/her name), etc. More attention needs to be given to understanding the harm that the Guidelines seek to prevent and/or mitigate. The real concern to the customer is that they may suffer actual financial loss, and/or detriment to their credit rating and reputation in the community. In addition, a case of stolen/compromised sensitive data may result in considerable embarrassment to a customer - and in of itself merit mandatory reporting.

Customer Notice

I am a little concerned that the requirement to alert customers, when an institution 'becomes aware'... unless...etc' is also imprecise. How is this level of awareness established after the fact? Who must become aware? The CIO/CSO, guy in the mailroom? There may be issues around when exactly the notification requirement has been triggered that perhaps should be teased out.

I am also concerned that the proviso allowing non notification is vague. What is 'an appropriate investigation'? Of what duration? Involving whom? If the institution is not equipped/sufficiently resourced or skilled to carry out the investigation, should a TP be engaged? In determining that misuse is 'unlikely to occur', what does this mean? It is my understanding that this is the current de facto reasoning used by many financial institutions when they fail to advise customers of incidents of unauthorized access. In my view this leaves considerable discretion to interpret the provisions in

accordance with short term cost considerations, which flies in the face of the intention of the Guidelines.

Other comments:

Banks increasingly moving from PKI/certs for online banking to one way SSL – new phishing attacks a concern here also. For SSL purposes, identification information often quite lax- mother's maiden name, favorite artist, DOB, etc, etc. Sensitive information should be any data required by a bank for a customer to enter site/online banking, and certainly SIN, drivers license - any combination of data identity thief can use to build false identity. There is a possibility that they could build this data over time - for instance an insider might take data piecemeal - perhaps not triggering reporting requirement in any one given instance- but combined effect over time is significant to the customer.

Zero liability policies are widely promoted by the banks to reassure potential online customers of the safety of the medium. However, there is a need for increased co-ordination/information sharing between institutions in cases of identity theft where customer 1 has sensitive data exposed at bank A and is then flagged as a debtor by bank B (where thieves rip off Bank B under customer 1's identity) – often customers are left hanging out to dry in these situations. Zero liability is useless here.

Surveys show concerns about identity theft making consumers more open to biometrics. FTC reports show consumers unhappy with banks concerning treatment they receive after id theft incidents.

Service Providers

There will be confusion about what level of oversight is required- strict audit rights? Compliance with BS7799 or a similar standard? Will service provider suffer same fate as banks in trying to determine when to notify as per comments above (except one step further removed from the customer). They may fail to notify banks for concerns about QoS commitments/penalties etc.

Corrective measures

Banks are very reluctant to cancel cards- huge expense involved. They often suggest to customer (in my experience) that 'they should decide' (the customer). However, mandatory cancellation may be prudent in given circumstances.

Other measures

Removing sensitive numbers from receipts – encrypting all/some digits. Moving like UK to CHIP and PIN.

Concerns

Organized crime etc have banks, TP clearing houses clearly in their sights. Per Symantec in early 2003, decrease in overall volume of attacks in second half of 2002, but sharp increase in volume/severity of attacks on financial services sector. Bugbear B virus/worm targeting sector.

Phantom withdrawal issues and ATMs. Banks forcing customers with disputed withdrawals to displace reverse presumption that ATMs secure – with skimming,

secret cameras, insider attacks, more such cases will arise. Difficult for customer to displace such a presumption, although attacks becoming more commonplace.

About Mary Kirwan

Mary Kirwan is an independent IT security & risk consultant and writer.

She is a member of the Irish Bar, and a qualified attorney in Canada and Australia. Ms. Kirwan has worked in the insurance industry, and as a civil and criminal lawyer. She has extensive experience in the IT security sector, having worked in many senior positions, while wearing several hats at once - from legal and regulatory affairs, to professional services, sales and marketing, PR, strategic management, and product development. She practiced as a commercial litigation counsel at a leading Canadian law firm in Toronto for several years, where she worked on a number of high profile commercial and international white collar crime cases and securities fraud, as well as practicing IP litigation, medical malpractice, media law, tax fraud and criminal law. She was also a Senior Federal Crown Attorney in the money laundering/narcotics division at the Department of Justice in Toronto, with a focus on wiretap cases. In addition, she was a member of the DoJ appellate court advocacy team. Ms. Kirwan has an Honors Degree in German and Irish from Trinity College Dublin, and a first class honors Masters Degree in Business from the Michael Smurfit Graduate School of Business at University College Dublin, with a specialty in Management Information Systems (MIS). Her thesis (1999) was on the topic of privacy and security as business enablers. She holds a Diploma in Information Security Management Principles from the British Computer Society, in addition to the Certified Information Systems Security Professional (CISSP) certification. She has taught e-security law to postgraduate law students, and e-strategy to MBA students. She was much in demand as a guest speaker in Ireland at academic institutions, including the Law Society of Ireland.

She actively participated in the European body responsible for drafting technical, legal and policy requirements for the EU Directive on E- Signatures, and has advised national governments on e-commerce/security legislative initiatives. She wrote a security focused web page for Baltimore Technologies that was well regarded and consulted by business, government, and the media. She is a member of the American Bar Association, and has contributed to a number of cyber security initiatives undertaken by that body. She has spoken at conferences around the world and appeared on radio and TV. She has been quoted in the Financial Mail on Sunday (UK), the International Herald Tribune, Internet World, New Scientist, the Globe and Mail, the National Post, Canadian Business Magazine, ComputerWorld, etc. She writes a monthly column for the Globe and Mail on IT, Security and Corporate Governance issues, and is completing a book on IT security and strategic initiatives for business, for broad release in the next few months.