Canadian Internet Policy and Public Interest Clinic
Clinique d'intérêt public et de politique d'internet du Canada

APPROACHES TO SECURITY BREACH NOTIFICATION:

A White Paper

January 9, 2007

Canadian Internet Policy and Public Interest Clinic (CIPPIC)
University of Ottawa, Faculty of Law
57 Louis Pasteur, Ottawa, ON K1N 6N5
tel: 613-562-5800 x2553
fax: 613-562-5417
www.cippic.ca

CIPPIC

The Canadian Internet Policy and Public Interest Clinic (CIPPIC) was established at the Faculty of Law, University of Ottawa, in 2003. CIPPIC's mission is to fill voids in law and public policy formation on issues arising from the use of new technologies. The clinic provides undergraduate and graduate law students with a hands-on educational experience in public interest research and advocacy, while fulfilling its mission of contributing effectively to the development of law and policy on emerging issues.

Canadian Internet Policy and Public Interest Clinic (CIPPIC)
University of Ottawa, Faculty of Law
57 Louis Pasteur, Ottawa, ON K1N 6N5
tel: 613-562-5800 x2553
fax: 613-562-5417
www.cippic.ca

Executive Summary

Identity theft and related fraud have become serious risks for individuals in the information age. Identity thieves gather sensitive personal information from a number of sources, then use it to engage in fraudulent activities in the name of the victim, usually for financial gain. Sources of information include data brokers and other organizations that collect, hold and disclose such information in the course of their normal activities. As the number and size of personal information databanks grows, security breaches exposing customer information to unauthorized access and use are becoming commonplace

Unless an organization notifies individuals whose information has been placed at risk, affected individuals may end up as the unwitting victims of potentially devastating identity theft. Yet organizations, especially those in competitive markets, have little incentive to disclose their security failures voluntarily, given the costs and the damage this can do to their reputation.

This White Paper argues for a Canadian law requiring that organizations notify individuals when their personal information has been compromised as a result of a breach of the organization's security. In particular, it calls for an amendment to the federal *Personal Information Protection and Electronic Documents Act* ("PIPEDA") to provide for mandatory notification of security breaches when certain types of personal information are exposed to unauthorized access as a result of a security breach.

Following a review of gaps in the Canadian legal framework, this Paper analyzes security breach legislation in the U.S., where over half the states have enacted a mandatory security breach disclosure requirement and where several federal bills are currently pending. Various arguments for and against mandatory notification are analyzed, and specific recommendations for amending PIPEDA are proposed.

TABLE OF CONTENTS

Page

Introduction

Identity theft and related fraud have become a serious problem in North America. Sometimes referred to as "the crime of the century", identity fraud offers low risks and high rewards for its perpetrators, combined with potentially high costs and devastating personal consequences for its victims.

In 2005, Phonebusters, a Canadian organization which studies and reports on identity theft, collects data, educates the public and assists Canadian and U.S. law enforcement agencies in consumer fraud cases, received over 12,000 complaints from victims of identity theft. The associated losses were an estimated $8.6 million. By October 2006, Phonebusters had received fewer complaints than in the previous year, but total losses had risen to almost $15 million.[1]

In the U.S., identity theft has topped the Federal Trade Commission's (FTC) list of consumer complaints for years. In 2004, the FTC received 246,570 identity theft complaints and in 2005, 255,565 complaints were recorded.[2] Between 2003 and 2005, approximately 9 million Americans were victims of identity theft annually.[3] In 2005, losses to victims and businesses were an estimated $56.6 billion.[4]

While thieves often gather information directly from individuals, they also reap valuable personal information from government and corporate databases. With advances in technology, organizations are collecting, storing and transferring more and more personal information about us as consumers, citizens, professionals, patients, employees, etc. This accumulation of vast amounts of personal information in large databanks increases the risks and impacts of unauthorized access to and use of personal information.

How should organizations deal with a security breach of personal information holdings? Should there be a legal requirement for the organization to notify the individuals whose personal information might be at risk? If so, how should this be done? Should every breach be the subject of notification or should there be a minimum threshold for notification?

These questions have received increasing attention in Canada and the U.S. in recent months, in light of high-profile security breaches[5] and a general mounting concern about

---

[1] The Canadian Anti-Fraud Call Centre (Phonebusters), *Monthly Summary Report* (October 2006).
[2] Federal Trade Commission, *Identity Theft Victim Complaint Data*, online: <http://www.ftc.gov>.
[3] State of California, Department of Consumer Affairs, *Recommended Practices on Notice of Security Breach Involving Personal Information*", (April 2006) at 5, online: http://www.privacyprotection.ca.gov/recommendations/secbreach.pdf [California Practices].
[4] *Ibid.*
[5] Leading the list of incidents prompting security breach notification laws is the infamous Choicepoint scandal in the U.S. in 2005. Knowing its database had been accessed by criminals, the giant data broker chose a minimalist approach, notifying only the 30,000 California residents affected, even though over

identity theft and related fraud. Sixty-eight percent (68%) of respondents to a recent Canadian survey felt that individuals and government agencies should be notified in the event of a data security breach.[6]

Recognizing that individuals need to know when their personal information has been put at risk in order to mitigate potential identity fraud damages, most states in the U.S. now have laws requiring that organizations notify affected individuals when a security breach exposes their personal information to unauthorized access. In contrast, neither the Canadian *Personal Information Protection and Electronic Documents Act*[7] (PIPEDA) nor corresponding provincial statutes include an explicit security breach notification requirement.

This White Paper considers the need for an explicit obligation in Canadian privacy law to notify affected individuals of a breach in an organization's security that places those individuals' personal information at risk. The Paper begins its analysis with a review of the existing Canadian legislative framework relating to security breach notification. It then analyzes security breach legislation in the United States, where over half the states have enacted a mandatory security breach disclosure requirement and where several federal bills are currently pending. The Paper then considers justifications for, and objections to, such legislation, before concluding with a series of recommendations for enacting an effective statutory obligation of security breach notification in Canada.

Relevant Canadian Law

A Canadian security breach notification obligation would supplement Canada's existing network of statutory and common law privacy laws. Arguably, information practices mandated by existing laws already require data breach notification under certain circumstances, but such a requirement is explicit in only one Canadian statute (Ontario's health privacy law).

Legislation

Private Sector

Every business in Canada that handles customer information is subject to the federal *Personal Information Protection and Electronic Documents Act* (PIPEDA) or its provincial equivalent in Alberta, British Columbia and Quebec. Under these statutes, businesses must implement safeguards to protect personal information against loss or theft, as well as against unauthorized access, disclosure, copying, use or modification.

100,000 individuals across the U.S. had been affected. California was the only state in the U.S. to require such notification at the time. Only after widespread public outcry were other individuals notified.

[6] EKOS Research Associates, "Identity Theft & Identity Management: Looking Through the Eyes of the Canadian Public", (Paper presented to the 7th Annual Privacy and Security Workshop, Toronto, 3 November 2006).

[7] *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c.5 (PIPEDA).

The form of required safeguards depends upon the sensitivity of the information. The more sensitive the information, the higher the level of protection required.

While there is no explicit requirement for security breach notification under PIPEDA or any of the three substantially similar provincial laws, such a requirement could be read into the general security obligations of each statute. Indeed, recent rulings by Privacy Commissioners in Alberta and B.C. (see below) suggest that breach notification may be implicitly required, in at least some circumstances, as an aspect of organizations' existing statutory security obligations.

The British Columbia and Ontario Privacy Commissioners jointly published a document in December 2006 entitled *Breach Notification Assessment Tool*.[8] This four page document is designed to assist organizations in determining (a) whether they need to notify individuals of the breach, (b) when and how they should go about such notification, (c) what to include in the notification, and (d) who else to inform of the breach. Interestingly, the Tool states in its introduction: "organizations that collect and hold personal information are responsible for notifying affected individuals when a privacy breach occurs." Despite this suggestion that organizations owe affected individuals the obligation to notify in the event of a breach, the use of the Tool is voluntary.

Also in December 2006, the B.C. Privacy Commissioner published *Key Steps in Responding to Privacy Breaches,* again with the aim of providing guidance to organizations facing a security breach that involves sensitive personal information.[9]

Two private member's bills requiring security breach notification have been introduced at the provincial level. In Ontario, Bill 174, the *Consumer Reporting Amendment Act*, was introduced by MLA Tony Ruprecht in 2005.[10] The Bill would make security breach notification mandatory for consumer reporting agencies and financial institutions. In Manitoba, Bill 204, the *Personal Information Protection and Identity Theft Prevention Act,* received first reading in December 2005.[11]

[8] Office of the Information and Privacy Commissioner for British Columbia and Information and Privacy Commissioner of Ontario, *Breach Notification Assessment Tool* (December 2006), online: <http://www.ipc.on.ca/images/Resources/up-ipc_bc_breach.pdf> and <http://www.oipc.bc.ca/pdfs/Policy/ipc_bc_ont_breach.pdf>.
[9] Office of the Information and Privacy Commissioner for British Columbia, *Key Steps in Responding to Privacy Breaches* (December 2006), online: <http://www.oipcbc.org/pdfs/Policy/Key_Steps_Privacy_Breaches_(Dec_2006).pdf>.
[10] *An Act to Amend the Consumer Reporting Act*, Bill 174 (Ontario, 38th Parliament), online: <http;//www.ontla.on.ca/library/bills/381/174381.htm>.
[11] *The Personal Information Protection and Identity Theft Protection Act*, Bill 204 (Manitoba, 38th Legislature): online <http://web2.gov.mb.ca/bills/sess/b200e.php>.

Public Sector

As with general private sector data protection legislation, none of the federal or provincial public sector privacy statutes includes an explicit data breach notification rule. However, such a requirement could possibly be read into the general security obligations applicable to governmental institutions.

The Ontario Information and Privacy Commissioner has issued guidelines for government organizations to follow in the event of a "privacy breach".[12] The guidelines recommend that individuals affected by the unauthorized disclosure of their personal information be notified of the breach, "barring exceptional circumstances". Notification should be by telephone or in writing, and individuals should be advised of the extent of the breach and the specifics of the personal information at issue. They should also be advised of the steps taken to address the breach, both immediate and long-term. The Information and Privacy Commissioner also recommends that it be notified in the event of a security breach.

Health Sector

Ontario's *Personal Health Information Protection Act, 2004* (PHIPA) is the only Canadian statute that establishes an unequivocal obligation to notify individuals if the security of their personal health information is breached.[13] The object of this statute is to protect the personal health information of Ontarians. "Personal health information" is defined broadly, to include "information that relates to the physical or mental health of the individual, including information that consists of the health history of the individual's family".[14]

Section 12 of PHIPA imposes a duty of care on health information custodians; they must "take steps that are reasonable in the circumstances to ensure that personal health information in the custodian's custody or control is protected against theft, loss and unauthorized use or disclosure and ensure that the records containing the information are protected against unauthorized copying, modification or disposal". Section 12 also imposes a duty on health information custodians to notify the owner of personal health information, at the first reasonable opportunity, if it is stolen, lost, or accessed by unauthorized persons.[15] This duty is subject to prescribed exceptions and restrictions.[16]

---

[12] Information and Privacy Commissioner of Ontario, *What to do if a privacy breach occurs: Guidelines for government organizations*, online: <http://www.ipc.on.ca/images/Resources/up-prbreach.pdf>.
[13] *Personal Health Information Protection Act*, S.O. 2004, c. 3, Sch. A (PHIPA).
[14] *Ibid.*, section 4.
[15] *Ibid.*, section 12.
[16] *Ibid.*; see, *e.g.*, s. 12(3) requiring researchers who possessed the information under s. 44(1) to go through the original data custodian to first obtain the permission to contact the individual whose data has been compromised.

The Ontario Privacy Commissioner has published guidelines for the health sector on how to fulfil their obligations under this section.[17]

Privacy Commissioner Investigations

Privacy Commissioners across Canada have released a number of decisions that suggest that, in certain circumstances, existing privacy laws may already require data breach notification.

Federal Privacy Commissioner

There are only a few investigations at the federal level which pertain directly or indirectly to security breaches. The closest cases deal with employee theft or the improper disclosure of personal information. These findings relate to the lack of proper data security practices rather than to the handling of security breaches *per se*, and none go so far as imposing a general duty to notify.

Alberta Privacy Commissioner

The Alberta Information and Privacy Commissioner engaged in four investigations in 2005/2006 concerning security breaches of personal information. In each case, personal information had been acquired by unauthorized persons, and in each instance, the Commissioner recommended that the organization notify affected individuals. These investigation reports suggest that the Alberta Commissioner considers breach notification to be an important moral responsibility, if not a legal duty, under the Alberta private sector data protection legislation.

In *Linens'N Things*, the complainant's credit card number had been used by a third party after being obtained in an unknown manner from a receipt.[18] The Commissioner concluded that sensitive customer personal information had not been disposed of in a secure manner. The company agreed that timely notification of customers affected was "critical to enable customers to take steps to protect themselves against the serious consequences of identity theft".[19]

In *Nor-Don Collection Network Inc. (NCN)*, the police recovered company records listing debtors' names and the amount of their respective debts from vacated premises. The personal information contained in these records included: name of debtor, address, home phone number, date of birth, Social Insurance Number, length of time at current address, own/rent status, amount of monthly rent/mortgage payment, occupation, name and

[17] Information and Privacy Commissioner of Ontario, *What to do When Faced with a Privacy Breach: Guidelines for the Health Sector*, online: <http://www.ipc.on.ca/images/Resources/up-hprivbreach.pdf>.
[18] Alberta Information and Privacy Commissioner, [2005] Investigation P2005-IR-001 (Report on an Investigation into the Security of Customer Information: Linen 'N Things), online: <http://www.oipc.ab.ca/ims/client/upload/P2005_IR_001.pdf>.
[19] *Ibid.*, at para.25.

address of employer, employer's phone number, length of time employed, monthly income, information about previous employers, bank name, branch, account number, account balances, value of assets and liabilities, net worth, etc.[20] The personal information in these records was more than enough for an identity thief to commit fraud in the names of these individuals. The Privacy Commissioner found that NCN had contravened section 34 of PIPA by failing to make reasonable arrangements to protect personal information in its custody. During the investigation by the Privacy Commissioner, NCN proposed to contact individuals affected by the security breach to 1) inform them they may be at risk for fraud; 2) provide information on actions taken to prevent such breaches in the future; and 3) offer assistance about how the individuals could protect themselves from identity theft.

In *Digital Communications Group Inc.*, the police recovered from unauthorized persons' cell phone contracts that contained personal information of individual subscribers. Security measures on the part of the cell phone company were found to be inadequate. The company worked with the Commissioner's office to develop a notification procedure for the 50 affected individuals and later provided confirmation that all had been contacted.[21]

In *Monarch Beauty Supply*, the police recovered financial information and customer credit card and debit card receipts from a confidential informant.[22] The police brought this to the attention of the Privacy Commissioner. During the Commissioner's investigation, an individual complained that the company involved had allowed a suspected criminal to access her credit card information and then use it for fraudulent purposes. In this investigation, the question of notification was front and centre. The company acknowledged that "timely notification of customers affected by the security breach is important to enable their customers to take steps to protect themselves against the serious consequences of fraud and identity theft".[23] The Commissioner made specific recommendations for actions that the company should take to notify and assist affected customers, including the contents of the notification letter, and recommended that the company contact affected credit card companies and financial institutions.

[20] Alberta Information and Privacy Commissioner, Investigation P2005-IR-002 (Report on an Investigation into the Security of Customer Information: Nor-Don Collection Network Inc.), online: <http://www.oipc.ab.ca/ims/client/upload/P2005_IR_002.pdf>.
[21] Alberta Information and Privacy Commissioner, [2005] A.I.P.C.D. No. 48, Investigation P2005-IR-003 (Report on an Investigation into the Security of Customer Information: Digital Communications Group Inc.), online: <http://www.oipc.ab.ca/ims/client/upload/P2005_IR_003.pdf>.
[22] Alberta Information and Privacy Commissioner, [2006] A.I.P.C.D. No. 8, Investigation No. P2006-IR-003 (Report on an Investigation into the Security of Customer Information: Monarch Beauty Supply [a division of Beauty Systems Group (Canada) Inc.]), online: <http://www.oipc.ab.ca/ims/client/upload/Investigation%20Report%20P2006_IR_003.pdf>.
[23] *Ibid.* at para. 43.

British Columbia Privacy Commissioner

Two 2006 investigations of security breaches by the B.C. Information and Privacy Commissioner addressed the issue of notification. In addressing breach notification issues, the Commissioner considered U.S. law and an Australian Privacy Commissioner investigation.

The first of these investigations concerned the purchase of computer tapes at a B.C. government auction.[24] The tapes contained extensive and sensitive personal information about thousands of residents. Several observers suggested that the government should give notice to each individual whose personal information had been disclosed. In his investigation, the Commissioner undertook an analysis of the California law requiring notification of security breaches and referred to an investigation of the Australian State of Victoria's Privacy Commissioner into the inappropriate disclosure of personal information from a database by the Office of Police Integrity. The Commissioner concluded that harm assessment should be the primary consideration in determining whether or not an organization should notify customers of a breach: "…the key (but not the sole) consideration overall should be whether notification is necessary in order to avoid or mitigate harm to an individual whose personal information has been disclosed".[25] He concluded that the B.C. *Freedom of Information and Protection of Privacy Act* did not require notification absent exceptional circumstances, but made no recommendations in this regard, and did not elaborate on such circumstances.

In a June 2006 investigation of a security breach by the Vancouver Coastal Health Authority (VCHA), the B.C. Commissioner acknowledged that "[o]ne of the underlying principles of privacy protection is that the individual have the opportunity to exercise a measure of control over their personal information … Notification was the only means by which a client could acquire a measure of control".[26] In this case, the VCHA had initiated a notification process on its own, so the issue of whether or not notification was required was not addressed. The Commissioner did, however, discuss the notification process and the difficulties encountered, and analyzed the outcomes in some detail. The Commissioner's report included an appendix entitled "Key Steps for Physicians in responding to Privacy Breaches". The Commissioner identified notification as a "key consideration" in breach situations, and stated that the obligation to notify is to be determined on a case-by-case basis using a risk assessment approach.

---

[24] Office of the Information and Privacy Commissioner for British Columbia, Investigation Report F06-01: Sale of Provincial Government Computer Tapes Containing Personal Information (31 March 2006), Quicklaw: [2006] B.C.I.P.C.D. No. 7, ss.3, 4, pp.25-29, online: <www.oipc.bc.ca/investigations/reports/investigationReportF06-01.pdf> [Report F06-01].
[25] *Ibid.* at 27.
[26] Office of the Information and Privacy Commissioner for British Columbia, Investigation Report F06-02: Investigation into Security of Personal Information Held by Vancouver Coastal Health Authority's Employee and Family Assistance Program (7 June 2006), online: <www.oipc.bc.ca/investigations/reports/InvestigationReportF06-02.pdf>.

Common Law

It is not clear if the common law imposes a duty to notify affected individuals in the event of a data security breach.[27] The existence of such a duty would likely derive from the theory that any compromise of personal information places an individual at increased risk of crimes such as identity theft.[28] In particular, the failure of a custodian of information to notify of a data breach deprives the affected individual of the opportunity to take steps to mitigate the risk or detect illegal use at the earliest opportunity.

It is also not clear if an increased risk of identity theft is enough of an injury or harm to be the foundation of a negligence claim. This is because liability in negligence generally requires that the plaintiff establish actual harm that is causally connected with the defendant's failure to meet an established standard of care. Further, such harm must be foreseeable. Even when the breach results in the fraudulent use of the individual's name or other personal information, damages may be hard to prove, as the financial institution concerned usually covers most or all of the immediate, tangible costs. Other costs (e.g., time and inconvenience, emotional anguish and loss of reputation on the part of the individual affected) are more difficult to prove and recover in court, but could conceivably form the basis for a damages claim.

To date, there is no Canadian caselaw relating to security breaches. However, a current class action lawsuit against the Canadian Imperial Bank of Commerce will require the court to address the issue of whether an increased risk of identity theft is in itself sufficient to establish the basis for a negligence claim against an information custodian, even if no fraud has occurred.[29] In time, it can be expected that an individual will bring a case in the Federal Court under PIPEDA seeking compensation from an information custodian for the theft or illegal use of personal information.

Application of U.S. Security Breach Legislation in Canada

Canadian businesses with American customers may have a statutory obligation to notify their U.S.-based customers in the event of a security breach. As discussed below, many U.S. states now have legislation making notification mandatory. The laws generally apply to custodians of information about residents of the particular state; however, there is no such limitation regarding the location of the custodian. Under the "real and substantial connection" test applied by Canadian courts in conflict of laws issues, a Canadian court could find sufficient connections between an American individual and a Canadian

[27] David T.S. Fraser, "Liability for Disclosure of Customer Information" vol. 6, no.3 (May 2006) at 1, online: <http://www.oba.org/en/pri/may06/Liability.aspx> [Fraser].
[28] *Ibid.*
[29] Docket 05-CV-283484CP (Ont. Sup. Ct.), online: <http://www.cacounsel.com/CIBC%Class%20Action%20Claim.pdf>. The plaintiffs claim that as a result of misdirected faxes, the bank should pay compensation to all affected individuals for the increased risk of identity theft, plus the cost of more vigilant credit monitoring.

information custodian to enforce in Canada a judgment under one of the American statutes.[30]

This possibility carries significant implications for those Canadian businesses having U.S. customers, especially those operating online. Applicable U.S. law may require them to report security breaches to affected customers in applicable U.S. jurisdictions. One wonders whether a company might therefore notify its American, but not Canadian, customers of the breach. Choicepoint's experience suggests that selective notification based on legal requirements may have negative public relations, financial and legal implications.[31]

Relevant United States Law

The American position on data breach notification is, paradoxically, much more developed than that of Canada. We say "paradoxically" because Canada's comprehensive commercial privacy legislation suggests a more developed privacy protection framework than the United States' patchwork of sectoral and issue-specific privacy laws. Well over half of U.S. states have enacted laws requiring customers to be notified when there is a data security breach.[32] This recent proliferation of state notification laws has led to efforts at the federal level to introduce a data breach notification law of general application that would pre-empt equivalent state laws.

Federal Legislation

The United States lacks a data breach notification law of general application. Financial institutions are, however, subject to obligations in this respect: the *Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice*, interpreting requirements under the *Gramm-Leach-Bliley Act*,[33] provides for data breach notification in the financial sector.[34] The Guidance requires that every financial

---

[30] *Ibid.*
[31] Choicepoint's reputation suffered greatly after its initial decision to notify only those individuals whom it was legally required to notify. The company was subsequently sued by many of its customers, was fined US$10 million by the Federal Trade Commission, saw a fall in its share values, and was called to account before the U.S. Congress.
[32] For inventories and reviews of state security breach notification legislation in the U.S. see Perkins Coie, *Data Breach Notification Chart* (21 December 2006), online: http://www.perkinscoie.com/statebreachchart/chart.pdf; Doug Markiewicz, *State Security Breach Legislation* (Pittsburgh, Penn.: VigilantMinds Inc., February 2006), online: <http://www.vigilantminds.com/files/vigilantminds_state_security_breach_legislation_ whitepaper.pdf>, [Markiewicz]; Consumers Union, *Notice of Security Breach State Laws* (27 June 2006), online: <http://www.consumersunion.org/campaigns/Breach_laws_May05.pdf>. See also Paul M. Schwartz & Edward J. Janger, "Notification of Data Security Breaches" (29 August 2006) Brooklyn Law School Legal Studies Research Paper Series, Accepted Paper No. 58, online: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=908709>.
[33] 15 U.S.C. 6801, s.501(b).
[34] Department of the Treasury, Federal Reserve System, Federal Deposit Insurance Corporation, *Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and*

institution have a response program that includes customer notification, in the event of a security breach.[35]

State Legislation

California was the first U.S. jurisdiction to enact security breach notification requirements. Incorporated into the *California Civil Code*, Senate Bill 1386 was introduced in 2002 and took effect in July 2003.[36] Focusing on "the privacy and financial security of individuals", California's statutory provisions apply to public sector agencies, as well as to businesses and persons doing business in the state (even if located outside the borders), who own or hold computerized data that includes personal information.

An ever-increasing number of states have followed California's lead in enacting breach notification legislation, with most states using the California legislation as a model, but departing from its approach on some issues. See the Appendix to this paper for a list of state laws. The following issues are addressed in many, if not most, statutes:

1. Trigger for Notification
    (a) Triggering Event
    (b) Definition of Personal Information
    (c) Encryption Exemption
    (d) Redaction Exemption
    (e) Risk of Harm Exemption
    (f) Exemption where already subject to similar federal law
2. Responsibility for Determining need for Notification
3. Responsibility for Notifying
4. Notification Method
5. Notification to other agencies
6. Notification Timelines
7. Security Freezes
8. Private Rights of Action

Trigger for Notification

The general rule for notification under most statutes is similar to that of California:

Customer Notice (effective 29 March 2005), online: <http://www.fdic.gov/news/news/financial/2005/fil2705a.pdf> [Interagency Guidance].

[35] Although not a federal law, the Interagency Guidance has legal weight. Under it, a financial institution's security program must include a response program that incorporates notification. If a program is considered to be insufficient, then informal or formal sanctions can be taken against the organization. In the case of a bank, for example, the Federal Deposit Insurance Corporation could issue a "cease and desist order" (Telephone conversation with Kathryn Weatherbee, Federal Deposit Insurance Corporation, 12 December 2006).

[36] SB 1386, codified at *California Civil Code*, ss. 1798.29, 1798.82-1798.84, online: <http://info.sen.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020926_chaptered.html> [Cal. Civil Code].

> "Any agency that owns or licenses computerized 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 unauthorized person*."[37] (emphasis added)

A central element of the notification obligation is the trigger: what event must occur to invoke an organization's obligation to notify? And what conditions exempt an organization from notifying in the event of what would otherwise require notification?

(a) Triggering Event

California and most other states treat "breach of the security of the system" as the triggering event, and define it as "*unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the agency*." This definition typically includes an exemption for harmless internal breaches such as: "*Good faith acquisition of personal information by an employee or agent of the agency for the purposes of the agency is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure*."[38]

Some states treat unauthorized *access to* the information as the trigger, either instead of or in addition to unauthorized *acquisition*.[39]

Note that under the general rule, *reasonable belief* that unauthorized acquisition has occurred as a result of the breach is sufficient to invoke the notification requirement.

(b) Definition of Personal Information

The California legislation defines "personal information" as:

> "an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:

---

[37] California Civil Code, *supra* note 36, s.1798.29(a).
[38] Ibíd., s.1798.29(d)
[39] *Connecticut Public Act* No. 05-148, s. 3, online: <http://www.cga.ct.gov/2005/act/Pa/2005PA-00148-R00SB-00650-PA.htm> [Connecticut Act]; *New Jersey Permanent Statutes*, s. 56:8-161, online: <http://lis.njleg.state.nj.us/cgi-bin/om_isapi.dll?clientID=128848&Depth=2&TD=WRAP&advquery=security%20breach&depth=4&expandheadings=on&headingswithhits=on&hitsperheading=on&infobase=statutes.nfo&rank=&record={175DF}&softpage=Doc_Frame_PG42&wordsaroundhits=2&zz=> [New Jersey Act].

> (1) Social security number.
> (2) Driver's license number or California Identification Card number.
> (3) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account."[40]

It excludes from that definition "publicly available information that is lawfully made available to the general public from federal, state, or local government records."[41]

Several states have taken California's approach but broadened the list of data elements which, when combined with a name (or other identifying information), are vulnerable to fraudulent uses. Other definitions include, for example:

- postal or mail address
- telephone number
- fingerprints or other unique biometric data
- certain types of medical information
- date of birth
- mother's maiden name
- account passwords
- passport number; state ID card; alien registration number
- employer or tax ID number
- Medicaid or food stamp account number
- unique electronic number, address or routing code
- telecommunication ID information or access device

Definitions adopted by North Dakota and North Carolina exhibit the greatest expansion in defining personal information. North Dakota defines "personal information" as follows:

> "2. a. "Personal information" means an individual's first name or initial and last name in combination with any of the following data elements, when the name and the data elements are not encrypted:
>
> > (1) The individual's social security number;
> > (2) The operator's license number assigned to an individual by the department of transportation under section 39-06-14;
> > (3) A nondriver color photo identification card number assigned to the individual by the department of transportation under section 39-06-03.1;
> > (4) The individual's financial institution account number, credit card number, or debit card number in combination with any required security code, access code or password that would permit access to an individual's financial accounts;
> > (5) The individual's date of birth;

[40] *California Civil Code*, s. 1798.29(e).
[41] *California Civil Code*, s. 1798.29(f).

> (6) The maiden name of the individual's mother;
> (7) An identification number assigned to the individual by the individual's employer; or
> (8) The individual's digitized or other electronic signature.
>
> b. "Personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records." [42]

Under North Carolina's statute, "personal information" means a person's first name or initial and last name, plus any of the following:

(1) SSN
(2) Drivers license numbers
(3) Checking account numbers
(4) Savings account numbers
(5) Credit card numbers
(6) Debit card numbers
(7) PIN
(8) Digital Signatures
(9) Any other numbers or information that can be used to access a person's financial resources
(10) Biometric data [or]
(11) Fingerprints[43]

Additionally, the North Carolina statute considers the following to be "personal information" if, when taken in conjunction with a person's first name or initial and last name, it "would permit access to a person's financial account or resources":

(1) Electronic ID numbers
(2) Email names or addresses
(3) Internet account numbers
(4) Internet ID names
(5) Parent's legal surname prior to marriage; or
(6) Passwords [44]

New York takes a slightly different approach, broadening the first part of the California definition (first name or initial and last name) to "any information concerning a natural person which, because of name, number, personal mark, or other identifier, can be used to identify such natural person".[45]

---

[42] *North Dakota Century Code* 51-30-01 *et. Seq*, online: <http://www.legis.nd.gov/cencode/t51c30.pdf>.
[43] North Carolina, S.B. 1048, online: <http://www.ncga.state.nc.us/Sessions/2005/Bills/Senate/HTML/S1048v1.html>.
[44] *Ibid.*
[45] New York, *Information Security Breach and Notification Act*, s. 899-AA, online: <http://www.cscic.state.ny.us/lib/laws/documents/899-aa.pdf> [New York Act]

The Interagency Guidance (applicable to financial institutions only) applies to breaches involving "sensitive customer information" which it defines as:

> "a customer's name, address, or telephone number, in conjunction with the customer's social security number, driver's license number, account number, credit or debit card number, or a personal identification number or password that would permit access to the customer's account. Sensitive customer information also includes any combination of components of customer information that would allow someone to log onto or access the customer's account, such as user name and password or password and account number."[46]

(c) Encryption Exemption

California and virtually every other state with a security breach notification law requires notification only for breaches involving unencrypted personal information.[47] New York requires notice for encrypted data, but only if the encryption key is also acquired by the thieves.[48] In contrast, the Interagency Guidance rejects a blanket exclusion for encrypted information because "there are many levels of encryption, some of which do not effectively protect customer information".[49]

The California statute does not define the term "encryption", leaving it up to organizations to determine what constitutes valid encryption under the statute. This provides latitude to organizations in selecting encryption applications that suit them and means that the security of encrypted information is dependent upon the strength of the cipher used for encryption and how well the encryption keys are protected.[50] To provide more guidance and protection for individuals, several states have defined encryption in their statutes.[51]

Maine's definition is the most simple: "disguising of data using generally accepted practices."[52] North Carolina, Ohio and Pennsylvania define encryption as "The use of an algorithmic process to transform data into a form in which the data is rendered

---

[46] Interagency Guidance, *supra* note 34.
[47] See, e.g., *California Civil Code*, s. 1798.29(a).
[48] New York Act, *supra* note 45.
[49] Interagency Guidance, *supra* note 34.
[50] *Ibid*., at 8. In April 2006, the California Office of Privacy Protection issued *Recommended Practices on Notice of Security Breach involving Personal Information* which includes the recommendation that "Data encryption should meet the National Institute of Standards and Technology's Advanced Encryption Standard". See California Practices, *supra* note 3, at 10.
[51] *Maine Revised Statutes*, s. 1347, online: <http://janus.state.me.us/legis/statutes/10/title10sec1347.html> [Maine Act]; *Nevada Revised Statutes*, s. 205.4742: online <http://www.leg.state.nv.us/NRS/NRS-205.html#NRS205Sec4742>; *North Carolina General Statutes*, s. 75-61, online: <http://www.ncga.state.nc.us/enactedlegislation/statutes/pdf/bysection/chapter_75/gs_75-61.pdf> [North Carolina Act]; *Ohio Revised Code*, s. 1347.12, online: <http://onlinedocs.andersonpublishing.com/oh/lpExt.dll?f=templates&fn=main-h.htm&cp=PORC> [Ohio Act]; Pennsylvania, *Breach of Personal Information Notification Act*, s. 2, online: <http://www2.legis.state.pa.us/WU01/LI/BI/BT/2005/0/SB0712P1410.pdf> [Pennsylvania Act].
[52] Maine Act, s*upra* note 51.

unreadable or unusable without use of a confidential process or key."[53] Nevada provides a more detailed definition:

> "the use of any protective or disruptive measure, including, without limitation, cryptography, enciphering, encoding or a computer contaminant, to:
>
> (1) prevent, impede, delay or disrupt access to any data, information, image, program, signal or sound;
> (2) cause or make any data, information, image, program, signal or sound;
> (3) prevent, impede, delay or disrupt the normal operation or use of any component, device, equipment, system or network."[54]

Other states avoid having to define encryption by exempting information that is unreadable as a result of any method or technology. For example, Connecticut requires notification only where "access to the personal information has not been secured by encryption or by any other method or technology that renders the personal information unreadable or unusable".[55] Ohio exempts information that is "altered by any method or technology in such a manner that the data elements are unreadable".[56] Similarly, the Nebraska exemption covers information that is "redacted, or otherwise altered by any method or technology in such a manner that the name or data elements are unreadable".[57]

(d) Redaction Exemption

Some states, such as Arizona, Illinois, Louisiana, Maine, Ohio, Nebraska, Pennsylvania, Vermont and Wisconsin exempt redacted as well as encrypted data from the scope of the disclosure rule.[58] As with "encrypted", the term "redacted" is not always defined, leading to uncertainty as to what type or extent of redaction eliminates the notification requirement.

The Pennsylvania[59] and Indiana[60] statutes define redacted information as truncating numerical identifiers so that no more than 4 or 5 digits are accessible. This form of redaction is mandated in some cases by other statutes. For example, the *Fair and*

---

[53] North Carolina Act; Ohio Act; Pennsylvania Act, *supra* note 51.
[54] Nevada S.B. 347, Chapter 485.
[55] Connecticut Act, *supra* note 39.
[56] Ohio Notice, *supra* note 51.
[57] Nebraska Notice, *ibid.*
[58] Illinois, *Personal Information Protection Act*, s. 5, online: <http://www.ilga.gov/legislation/publicacts/fulltext.asp?Name=094-0036>; *Louisiana Revised Statutes*, s. 3073, online: <http://www.legis.state.la.us/lss/lss.asp?doc=322029>; *Maine Revised Statutes*, s. 1347 Act, *supra* note 51; Ohio Act, *supra* note 51; Nebraska, *Financial Data Protection and Consumer Notification of Data Security Breach Act of 2006*, s. 2, online: <http://www.unicam.state.ne.us/pdf/FINAL_LB876_2.pdf>; Pennsylvania Act, *supra* note 51; *Vermont Statutes*, s. 2430, online: <http://www.leg.state.vt.us/statutes/fullchapter.cfm?Title=09&Chapter=062>; *Wisconsin Statutes*, s. 895.507. online: <http://www.legis.state.wi.us/statutes/Stat0895.pdf>.
[59] Pennsylvania Act, *supra* note 51.
[60] *Indiana Code*, s. 24-4.9-2-11, online: <http://www.in.gov/legislative/ic/code/title24/ar4.9/ch2.html>.

Accurate Credit Transactions Act (FACTA), U.S.C. § 1681, requires truncation of credit card numbers that are printed on receipts.[61] Section 1747.09 of the *California Civil Code* imposes a similar duty.[62]

(e) Risk of Harm Exemption

Many states, including Alabama, Arkansas, Connecticut, Delaware, Florida, Louisiana, New Jersey, North Carolina, Pennsylvania and Rhode Island, apply a "risk of harm exemption" that releases an organization from its disclosure obligation if, after a "reasonable investigation" (which may require consultation with relevant federal, state and local agencies responsible for law enforcement), the entity reasonably determines that the breach will not likely result in harm to the individuals whose personal information has been compromised.[63] Most such statutes define neither "reasonable investigation" nor "harm", thus leaving scope for interpretation.

Vermont provides that notice need not be given if the data collector establishes that misuse is not reasonably possible, and provides notice and an explanation to the Attorney General or to the department of banking, insurance, securities and health care administration, as applicable.[64]

Similarly, the Interagency Guidance applies a test of actual or likely *misuse* of personal information as a result of the breach. It requires that a financial institution notify affected customers if it determines that "misuse of its information about a customer has occurred or is reasonably possible".[65]

In contrast, New York's law requires that companies disclose all data breaches that meet other threshold requirements, even if the company concerned assesses the risk to consumers as minimal.[66]

(f) Exemption where organization already subject to similar federal law

Several states exclude from the scope of the notification requirement financial institutions that are bound to related requirements of the *Gramm-Leach-Bliley Act* (GLBA). The GLBA requires that financial institutions ensure that their customer records are protected from unauthorized access or use.[67] While the GLBA does not include an explicit security breach notification requirement, the *Interagency Guidance* clarifies the responsibilities of

[61] *Fair and Accurate Credit Transactions Act* (FACTA), U.S.C. § 1681, online: <http://www.ftc.gov/os/statutes/031224fcra.pdf>.
[62] *California Civil Code*, online: <http://www.leginfo.ca.gov/cgi-bin/calawquery?codesection=civ&codebody=&hits=20>.
[63] See, *e.g., Kansas Bill* S.B. 196, s. 4, online: <http://www.kslegislature.org/bills/2006/196.pdf>.
[64] Vermont Act, *supra* note 58.
[65] Interagency Guidance, *supra* note 34 at 14.
[66] New York Act, *supra* note 45.
[67] *Gramm-Leach-Bliley Act*, s. 501,online: <http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=106_cong_public_laws&docid=f:publ102.106.pdf>.

financial institutions under this Act.[68] As noted above, the Guidance requires that financial institutions have a response program for incidents of unauthorised access to customer information that includes timely and effective breach notification. The Guidance describes customer notification as an "important tool" in enabling a customer to take steps to prevent identity theft, and sets out the particulars of breach notification in some detail.

Responsibility for Determining need for Notification

All state statutes, as well as the Interagency Guidance, place responsibility for deciding whether notification is required following a security breach on the organization itself.[69] We have not identified any U.S. statutes that give responsibility for this determination to another agency or authority.

Responsibility for Notifying

Some states apply notification obligations not only to persons who own or license computerized data, but also to those who acquire, handle, collect, disseminate or otherwise deal with non public personal information.[70] California, on the other hand, makes a distinction between an entity that owns or licenses data and an entity that merely maintains data, and places responsibility for notifying customers following a security breach solely in the hands of the entity that owns or licenses data.[71]

Notification Method

Under the California law, notice may be provided in written, electronic, or substitute form depending on whether the criteria for each are met.[72] For electronic notification to be valid, the consumer must have consented to receipt of electronic notice. [73] Several states permit telephone notice, in addition to notice by mail, as a primary form of notification.[74]

Most states have developed a substitute notice regime to handle large security breaches. In California, substitute notice can be used if the cost to provide written or electronic notice exceeds $250,000 or if more than 500,000 consumers are impacted.[75] Substitute notice requires (1) email notice if an email address is on file, (2) conspicuous posting on the entity's website, and (3) notification of major state-wide media. Substitute notice by email does not require advance consent from the consumer – it is merely a good faith

[68] Interagency Guidance, *supra* note 34 at 16.
[69] *California Civil Code*, s. 1798.29(a) and (b), and 1798.82(a) and (b).
[70] See, for example *Delaware Code*, s. 12B-102(b),online: <http://www.delcode.state.de.us/title6/c012b/index.htm> [Delaware Act].
[71] *California Civil Code*, s. 1798.29(a).
[72] *California Civil Code*, s. 1798.29(g) and 1798.82(g).
[73] *California Civil Code*, s. 1798.29(g)(2), 1798.82(g)(2) and 15 U.S.C. § 7001.
[74] For example, Ohio Act, *supra* note 51and Delaware Act, *supra* note 70.
[75] *California Civil Code*, s. 1798.29(g)(3), 1798.82(g)(3).

attempt at providing email notification. Under Delaware law, substitute notice can be used if the cost of the primary forms of notification exceeds $75,000 or if the number of affected consumers exceeds 100,000.[76] At the other end of the spectrum, Maine applies $5,000 or 1,000 consumers as its threshold for substitute notice.[77]

Notification to other agencies

A number of states require that organizations notify consumer reporting agencies in the event that the breach affects a statutorily mandated number of people (ranging from 500 to 10,000).[78]

In New York, organizations must also notify the state Attorney General (who can bring an action on behalf of New York citizens for contravention of the breach notification law), the Consumer Protection Board, and the State Office of Cyber Security and Critical Infrastructure Coordination of the approximate number of affected individuals and the timing, content, and distribution of notices.[79] In North Carolina, the Consumer Protection Division of the Attorney General's Office must be notified if more than 1,000 persons are affected.[80]

Notification Timelines

Florida and Ohio require notification to be made within 45 days of the security breach.[81] Most other states do not apply a set time period for notification; rather, they follow the more flexible California approach, leaving room for longer timelines where appropriate in the circumstances. The California law states:

> "The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement [...] or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system." [82]

Most states permit delay of notification in order not to impede a criminal investigation or to allow for cooperation with a law enforcement agency.[83] This determination is usually to be made by law enforcement officials, not the company. In addition, North Carolina and Ohio provide that notification can be delayed if it would jeopardize national security.[84]

---

[76] Delaware Act, *supra* note 70.
[77] Maine Act, *supra* note 51.
[78] For example, see Maine, New York and North Carolina Acts, *supra* notes 51, 45 and 51.
[79] New York Act, *supra* note 45.
[80] North Carolina Act, *supra* note 51.
[81] *Florida Statutes*, s.817.5681(1)(a): online <http://www.leg.state.fl.us/statutes/> and Ohio Act, *supra* note 51.
[82] *California Civil Code*, s. 1798.29(a).
[83] See, e.g., *California Civil Code*, s. 1798.29(a) and (c); Illinois Act, *supra* note 58.
[84] North Carolina and Ohio Acts, *supra* note 51.

Security Freezes

Connecticut, New Jersey and North Carolina have included provisions allowing consumers to place a freeze on their credit report if they have been notified of a security breach affecting their personal information.[85] Security freeze provisions typically require a consumer to submit a security freeze request to credit reporting agencies. Upon establishment of the security freeze, all requests for release of credit information to a third party must first be authorized by the consumer. Some provisions set out or limit fees that consumer reporting agencies may charge for security freezes (e.g., no more than $10 for adding or removing a security freeze and $12 for temporarily lifting a security freeze,[86] or no fee permitted for initiation of a security freeze[87]).

Private Rights of Action

The majority of state laws, as well as the Interagency Guidance, do not make express provision for a private right of action. Among those that do provide for a private right of action, Louisiana, Maine, and North Carolina require proof of injury.[88] Maine provides for one or more of civil penalties of $500 per violation, to a maximum of $2500 per day, equitable relief or enjoinment from future violations.[89] Nevada allows a data collector who provides breach notification to bring an action for damages against anyone who unlawfully obtained or benefited from the records of the collector.[90] The courts can order restitution be paid to the data collector for reasonable costs incurred in providing notification of the breach.[91]

Proposed U.S. Federal Legislation

As noted above, the proliferation of different state approaches to data breach notification has prompted a number of initiatives to design a comprehensive federal legislative framework for security breach notification.[92] A federal law would pre-empt most state laws and thus standardize approaches to data breach notification.

---

[85] Connecticut Act, *supra* note 39, s. 2; New Jersey Act, *supra* note 39, s. 56:11-46.5.a; and North Carolina Act, *supra* note 51.
[86] Connecticut Act, *supra* note 39, s. 2(h)(i).
[87] New Jersey Act, *supra* note 39, s. 56:11-46.5.m.(1).
[88] *Louisiana Revised Statutes*, s. 51:3075, online: <http://www.legis.state.la.us/lss/lss.asp?doc=322031>; Maine Revised Statutes, s. 1349.2, online: <http://janus.state.me.us/legis/statutes/10/title10sec1349.html> [Maine Penalties]; North Carolina Act, *supra* note 51.
[89] Maine Penalties, *supra* note 88, s. 1349.2.
[90] *Nevada Revised Statutes*, s. 603A.900, online: <http://www.leg.state.nv.us/NRS/NRS-603A.html#NRS603ASec900>.
[91] *Ibid.*
[92] *Financial Data Protection Act of 2006*, Bill H.R. 3997, online: <http://www.govtrack.us/data/us/bills.text/109/h/h3997.pdf>; *Data Accountability and Trust Act* (DATA), Bill H.R. 4127: online <http://www.govtrack.us/data/us/bills.text/109/h/h4127.pdf>; *Identity Theft Protection Act*, Bill S. 1408, online: <http://www.govtrack.us/data/us/bills.text/109/s/s1408.pdf>; *Personal*

The four federal bills under consideration as of December 2006 propose a variety of approaches, including more stringent notification requirements, broadened scope of disclosure, eliminating the "encryption safe harbour", creating additional agencies within the federal government to combat identity theft and oversee statutory compliance, and requiring companies to provide additional notices to credit reporting agencies and certain designated federal agencies.[93] For the most part, the bills put the burden on law enforcement agencies to request a delay in notification, and only one of the federal bills offers a risk-of-harm exemption.[94] It remains to be seen which, if any, of the bills will be enacted into law and which notification provisions will be adopted.

U.S. Caselaw

A number of lawsuits relating to security breaches have been filed in the U.S.[95] Companies sued have included Choicepoint, LexisNexis and CardSystems Solutions Inc.[96] Seven actions were initiated by government agencies, including five by the FTC and two by the New York Attorney General.[97] Eight others, of which six were still pending in May 2006, are class actions or attempted class actions.[98] Private actions have been filed in relation to security breaches in Maine and Ohio, claiming breach of contract, negligence and/or unfair or deceptive acts.[99]

Syran v. LexisNexis was filed on behalf of 35,000 California residents and 110,000 non-residents. Its claims include negligence on the part of the company for disclosing consumer reports to affiliates that had no permissible purpose for their receipt or use.[100] In *Parke v. CardSystems Solutions Inc.*, it is alleged that the company failed to implement and maintain reasonable security measures and failed to disclose a security breach as required by the California law.[101]

As of December 2006, none of these actions had reached judgment.

Data Privacy and Security Act of 2005, Bill S.1789, online: <http://www.govtrack.us/data/us/bills.text/109/s/s1789.pdf> [S.1789].
[93] *Ibid.*
[94] S. 1789, *supra* note 92, s. 322(b).
[95] Privacy and American Business, "Personal Data Security: Actions for Breaches" (May 2006) *Consumer Privacy Litigation Report.*
[96] David Bender, "Security Breach Notification Laws and FTC Activity Induce Enhanced Security" (April 2006) 23 (No. 4) *The Computer & Internet Lawyer* at 1.
[97] Center for Social & Legal Research (13 July 2006) *Personal Data Security: Actions for Breaches.*
[98] *Ibid.*
[99] *Ibid.*
[100] *Ibid.*
[101] *Ibid.*

Relevant Australian Law

Australia, like Canada, does not have an explicit security breach notification requirement in its data protection legislation. The Australian Privacy Commissioner has recommended a review of the federal *Privacy Act* (which covers public and private sectors) to look at privacy risks posed by new technologies and advises voluntary reporting of security breaches as "good privacy practice" for companies, but has not proposed an explicit breach notification law as in the United States.[102]

Not all Australians are satisfied, however, with reliance on voluntary disclosure by companies holding databases of personal information. One expert has argued that Australia needs security breach notification legislation, with stiff penalties, stating:

> "Many companies in Australia are playing Russian roulette with their customers' data. If the gun had all the chambers loaded and it was pointed at the head of the CEO, we'd see pretty fast changes in the way companies protect our personal data…If a company based in Australia had its database of customers' personal data breached, and some of these customers were based in the U.S., it would seem extraordinary if the U.S. did not insist on the breach being disclosed to those affected…(Australian regulators would have to)…take a good look at why we were telling U.S. citizens but not our own…"[103]

The Privacy Commissioner for the State of Victoria, in his investigation of inappropriate disclosure of personal information by the Office of Police Integrity (a civilian oversight body for police conduct) stated that the *Privacy Act* contains a "presumption … that privacy breaches ought to be notified to those whom they potentially affect".[104]

The Case for a Legal Duty to Notify

According to a July 2006 national survey, a large majority of Canadians (68%) think that organizations should notify both individuals and government agencies in the event of a data security breach.[105] Clearly, this is an issue that resonates with the public in Canada as well as in the United States. Debate is shifting from the general appropriateness of mandatory notification regimes to the appropriate level of discretion that organizations should have in determining whether, when, and how to provide such notification.

---

[102] Privacy Commissioner of Australia, Report F06-01.
[103] Data Theft Awareness (14 September 2005) "Data protection laws on ice", online: http://www.datatheft.org/2005/09/data_protection_laws_on_ice.html.
[104] Privacy Commissioner, State of Victoria (February 2006) Report 01.06: "Jenny's case: Report of an investigation into the Office of Police Integrity pursuant to Part 6 of the Information Privacy Act 2000", para. 9.3.1 at 65.
[105] EKOS Research Associates, *supra* note 6.

Perhaps reflecting the relatively recent enactment of breach notification laws, there is little research assessing their effectiveness in either reducing identity fraud or in preventing breaches in the first place. While it is hard to know how many breaches have been prevented and to what extent harm has been reduced as a result of these laws, it can reasonably be assumed that the existence of such laws has been a catalyst for organizations to tighten up their information security practices. As one commentator has said,

> "what these data notification statutes have done is to put every Chief Executive Officer (CEO) on notice that, if he or she does not want to read about his or her company's breach on the front page of USA Today, the company had better bring its security up to snuff".[106]

Breach notification laws clearly provide organizations with an incentive to improve security. Organizations will surely take greater care to prevent security breaches if they know that such breaches will carry significant costs in terms of reporting and negative publicity. Conversely, "the ability to cover up data security breaches simply encourages complacency and rewards incompetence."[107]

The other rationale for breach notification laws is that individuals whose personal information has been exposed to potential unauthorized use as a result of a security breach deserve to be notified so that they can take measures to protect themselves against identity fraud. Failure to warn individuals of the potential for identity fraud, once an organization is aware of that potential and has the means to notify those affected, is arguably negligent and irresponsible.

Critics, on the other hand, argue that security breach notification laws can create unnecessary and burdensome costs, not only for organizations but also for consumers, who may take unnecessary protective measures as a result of the notification. One commentator argues that the probability of a single breached account being misused is very small (from 1% to 5%), leading to possible over-notification and undue alarm on the part of some individuals.[108] A September 2006 U.S. study by Javelin Strategy and Research concluded that data breaches were responsible for only 6% of all known cases of ID fraud in both new and existing accounts over the past year.[109]

These estimates were put into question by a more recent HarrisInteractive poll indicating that, of the estimated 49 million Americans who were notified of unauthorized access to their personal information during the past three years, 19% (app. 9.3 million people)

---

[106] Quoted in Raf Brusilow, "Lax security leaves your data open to thieves" *Globe and Mail* (8 November 2006) at B13.
[107] Mary Kirwan, "Is no news really good news?", *Globe and Mail Update* (3 Jan.3 2007).
[108] Michael Turner, "Towards a Rational Personal Data Breach Notification Regime", Information Policy Institute (June 2006) at 3, online: <http://www.infopolicy.org/pdf/data-breach.pdf>.
[109] Javelin Strategy and Research (September 2006) *Data Breach/Identity Theft Study*, online: <http://www.finextra.com/fullstory.asp?id=15860>.

believe that something harmful happened to them as a result of the breach.[110] Such harm included merchandise charged in their name (43%), some kind of fraud costing them money (35%), money taken from their bank account (18%), a credit card taken out in their name (11%), or someone posing as them to get a benefit or service (8%). Thus, the benefits of notification appear to be much higher than critics have estimated.

Perhaps acknowledging that the benefits of well-designed notification regimes can outweigh the costs, many critics focus less on whether mandatory notification is a good idea, and more on the test for notification. Businesses, they argue, should be empowered to determine themselves whether the risk of harm warrants notification, as well as who should be notified, and when and how.[111] However, even critics of breach notification laws acknowledge that organizations have no market incentive to report breaches that would otherwise remain undetected by the public.

> "A firm may not have an incentive to notify consumers of breaches when the cost of the notification exceeds the expected damage to the firm. That is, even if the costs of notifying a customer is smaller than the damage that will be mitigated, a firm has no incentive to bear this cost if the damage it will be spared is less than the costs of telling the consumer. […] Second a firm may run the risk of damage as a result of notification itself. Reputational damage has been mentioned, but a firm also faces the risk of legal action…"[112]

There can be no question that, if they are legally obligated to report security breaches and thus to incur related reputational and business costs, organizations will be more inclined to ensure better security measures and thus to prevent breaches from occurring in the first place.[113] Indeed, mandatory breach notification requirements, in addition to empowering individuals to protect themselves from identity fraud, should have a general beneficial effect on organizations' data security practices.

In addition, there can be no doubt that without notification of breaches affecting their personal privacy, individuals cannot take targeted measures to prevent related fraud.

For these reasons, CIPPIC advocates the enactment of a data breach notification law. Such a law should be standardized across the country to the extent possible, so that businesses are not subject to different obligations depending on the province. It should be structured so as to achieve the goal of minimizing identity fraud without undue cost to business, government or individuals.

---

[110] HarrisInteractive News Release, "Many U.S. Adults Claim to Have Been Notified that Personal Information has been Improperly Disclosed" (6 November 2006).
[111] Thomas Lenard and Paul Rubin, "An Economic Analysis of Notification Requirements for Data Security Breaches" (July 2005) The Progress Freedom Foundation, Release 12 at 3.
[112] Michael Turner, *supra* note 108 at 12.
[113] David Bender, supra note 96 at 1; Paul M. Schwartz & Edward J. Janger, supra note 32 at 39.

Recommendations for a Canadian Breach Notification Law

Amend PIPEDA to include an explicit security breach notification requirement

In a submission dated November 28, 2006 to the House of Commons Standing Committee on Access to Information, Privacy and Ethics in its review of the *Personal Information Protection and Electronic Documents Act*, CIPPIC made the following general recommendation:

> *Amend Principle 7 of PIPEDA to include a requirement to notify affected individuals of a security breach that results in the acquisition of unencrypted personal information by an unauthorized person. Such requirement should include specifics regarding the type of personal information and breach that triggers the obligation to notify, form and content of notices, timing of notices, who should be notified, etc. Failure to notify affected individuals as required under the Act should be subject to tough penalties.*

In order to minimize cost to businesses, legal requirements for security breach notification should be uniform across Canada. For this reason, we recommend using the federal data protection law, PIPEDA, as the vehicle for an explicit security breach notification requirement. Substantially similar provincial legislation should also be amended accordingly, in order to maintain their substantially similar status.

Breach Notification Trigger and Risk Assessment

> *Notification should be required when designated personal information has been, or is reasonably believed to have been, acquired by an unauthorized person. Good faith acquisition of personal information by an employee or agent of the agency for the purposes of the agency should not trigger the notification requirement, provided that the personal information is not used or subject to further unauthorized disclosure*."

We recommend adoption of the threshold applied in California and many other states in the U.S.: acquisition, or reasonable belief of acquisition, by an unauthorized person. This standard is higher than mere "access by an unauthorized person", but lower than standards that incorporate a "risk of identity fraud" element. We believe that, together with the proposed definitions below, it properly balances the competing interests at play.

> *An "**unauthorized person**" means:*
> *a) A person who is not an employee or agent of the person that maintains the designated personal information;*
> *b) An employee or an agent of the person that maintains the designated personal information who*
> *(i) exceeds his or her authority to access the designated personal information; or*

(ii) uses the information for purposes not related to his or her duties.

*"**Designated personal information**" is information, in electronic or paper form, which includes the first name, initial, or middle name, and last name, or address, in combination with any of the following data: government issued identification number including social insurance number, driver's license number, or health card number; account numbers, credit or debit card numbers, or other unique identifiers issued by other organizations together with any security code, password or access code that would permit access to the individual's information.*

Information that is encrypted, redacted, or otherwise altered by any method or technology in such a manner that the name or data elements are unreadable by unauthorized persons does not constitute "designated personal information".

The definition of "designated personal information" includes the combination of mere address and other sensitive information because it is relatively easy to obtain a person's name from an address, using phone books, online databases and search engines.

The trigger for notification should be based on an objective test applied by organizations and subject to review by the applicable Privacy Commissioner. The test should be designed to avoid notification obligations where the breach does not expose individuals to a real risk of identity theft, but to apply in all situations where such a risk is created.

Commercial organizations might prefer to limit the scope of actionable security breaches to those generating a "significant risk of identity theft or fraud". However, such a threshold is difficult to apply objectively, and if applied subjectively, leaves too much discretion in the hands of organizations with a vested interest in secrecy. Not surprisingly, it has generally been rejected in U.S. state laws.

Some organizations have raised the spectre of over-notification if the notification trigger is not limited by the presence of a "high risk" requirement. According to this theory, if the trigger for notification is too wide, individuals may become desensitized to the notices and will eventually ignore notices altogether. However, in various surveys, individuals have indicated that they wish to receive more information on security breaches and have the opportunity to take protective measures as they see fit.[114] Moreover, the exercise of notification serves to document the problem that occurred and can help organizations mitigate the risk in the future.[115] Finally desensitization can be minimized by providing individuals with a risk assessment in the notification itself.

Organizations should have the responsibility for determining whether or not the standard for data breach notification is met.

[114] Ponemon Institute (26 September 2005) *National Survey on Data Security Breach Notification* at 3 and 9 and FTC/Synovate, *Identity Theft Survey Report*" (Washington, D.C., September 2003) at 63.

Generally, the affected organization is in the best position to calculate the associated risks of a breach of its information security and should be entrusted with this determination. However, there should be a requirement that every breach involving defined personal information be reported to the Privacy Commissioner, with full information about the nature and extent, the anticipated risks, mitigation measures, steps taken to notify affected individuals or, where notification is not considered warranted, the justification for not taking this step. (See below)

Who should be notified?

> *Notification of security breaches should be made to affected individuals, the owners of personal information, the Privacy Commissioner, government agencies, credit bureaus and law enforcement authorities. The Privacy Commissioner should be notified within five (5) business days of the security breach.*

Affected individuals

Notice should be given to every person whose personal information has been compromised by the security breach. If it is not possible to identify individuals who have been affected by the breach, all those likely to be affected should be notified.

Organizations on behalf of whom the information was being held

If an organization maintains (the "maintainer") information on behalf of another organization, the maintainer should notify the other organization of the security breach. The other organization should have responsibility for notifying affected individuals and for indicating that the maintainer is the source of the breach. If two or more organizations are unable to come to an understanding as to which one has responsibility for notification, the organization that suffered the security breach should notify the affected individuals.

Privacy Commissioner

Notice of all security breaches should be made to the Privacy Commissioner within five business days of discovery of the breach, irrespective of whether the test for individual notification is met. Notifying the Privacy Commissioner ensures that a record is kept of all security breaches involving personal data, allows for oversight of organization practices, and offers the potential for organizations to obtain guidance from the Privacy Commissioner regarding notification obligations and methods.

Credit Bureaus

Canadian credit bureaus should be notified of security breaches as a matter of course, so they can monitor account activity and take steps to ensure that the privacy and credit rating of affected individuals are protected.

Government Agencies

Federal and provincial agencies, especially those that issue identification documents such as passports, Social Insurance Numbers and drivers licenses, should be notified of security breaches, as appropriate in the circumstances. The Privacy Commissioner may give guidance to organizations as to which agencies should be notified in the context of a specific breach.

Law Enforcement Agencies

The Royal Canadian Mounted Police (RCMP) and other law enforcement authorities as appropriate should be notified of security breaches.

Form and Content of the Notice

> *Security breach notices should be separate from other communications and should include detailed information about the breach, including an assessment of the risk that the personal information of affected individuals will be used in an unauthorized manner.*

Form of the Notice

To avoid any confusion, the notice should be a stand-alone communication. Notification should not be combined with another communication, such as account statements or marketing materials.

Contents of the Notice

Notices should include the following information:

- a general description of what occurred;
- the date and time of the breach (or the best possible estimate);
- the date and time the breach was discovered;
- the source of the breach (either the organization itself or the third party that maintained information on its behalf);
- a list of the type of personal information disclosed;
- an assessment of the risk of identity fraud as a result of the breach;
- a description of the measures taken or that will be taken to prevent further unauthorized access to personal information;
- contact information for affected individuals to obtain more information and assistance; and
- information and advice on what individuals can do to protect themselves against identity theft and fraud.

Risk Assessment

The risk assessment should include a simple rating of the risk such as "high", "medium" or "low". Organizations can further qualify this rating by providing more information.

Information on How to Protect Against ID Fraud

The legislation should prescribe specific minimum information that must be provided to individuals regarding what they can do to protect themselves from identity fraud arising from the breach.

Timing of the Notice

> *Security breach notification should be undertaken as soon as possible and without unreasonable delay after the occurrence of the breach, except where a law enforcement agency has made a written request for a delay. Delays for law enforcement purposes should be for specified periods of time, and for no longer than 60 days at a time.*

Any delay for law enforcement purposes should be permitted only where the RCMP or other law enforcement authorities have requested such delay in writing. Such delays should not exceed 60 days. The 60 day period could be extended if a delay is requested by the RCMP or other law enforcement authorities for investigative purposes.

Mode of notification

> *Notification should generally be by regular mail, but electronic and substitute notice should be permitted when certain conditions are met. Email notification should be permitted only if the individual concerned has consented explicitly to receiving important notices such as this by email. Substitute notice should be permitted where large numbers of individuals (e.g.,100,000) must be notified, where the total cost of individual notification is extraordinary (e.g., over $150,000), or where the Privacy Commissioner has specifically approved the substitute notice.*
>
> *The cost of notification should be borne by the organization that incurred the security breach.*

By Mail

Security breach notices should, as a matter of course, be sent by mail to affected individuals.

By Email

Consent to receiving marketing communications by email, for example, does not constitute consent to receiving important notices by email.

Substitute Notification

Possible substitute mechanisms include:
- telephone, fax or email;
- posting the notice conspicuously on the home page of the website and on login screens used by users to access their accounts on the company's website; and/or
- notifying major provincial media in each province where affected individuals reside.

Application to the Privacy Commissioner for substitute notice should include details on the proposed method of notice. The Privacy Commissioner should be empowered to require that a specific mechanism or a combination of mechanisms be used in order to ensure the efficacy of the notification.

Role of Privacy Commissioner

> *The Privacy Commissioner should keep records of all security breaches of which it receives notice, should provide guidance to organizations collectively and individually as appropriate, and should take an active role in raising public and organizational awareness about security breaches. The Commissioner should also be empowered to order notification and substitute notice in appropriate cases.*

Receive and Review Information about all Security Breaches

The Privacy Commissioner should be responsible for reviewing all reports of security breaches, and for ordering notification or substitute methods of notification where appropriate.

Compile statistics on security breaches

The collection of statistics by the Privacy Commissioner will assist in assessing the effectiveness of notification requirements and the progress of organizations over time.

Develop Expertise

By compiling statistics and by participating at various stages of the security breach notification process, the Privacy Commissioner will develop expertise in the area of security breaches. This expertise can be shared with organizations to help them in their efforts to combat security breaches.

Oversight

The Privacy Commissioner also has an important oversight function. The Privacy Commissioner should have the power to mandate that organizations take steps in order to prevent future security breaches.

Compel information disclosure

In order to accomplish its important role, the Privacy Commissioner should have the power to compel organizations to provide information on security breaches.

Penalties and Enforcement

> *Failure to notify individuals and organizations as required under the new law, as well as failure to comply with a Commissioner order under the law, should be treated as offences under PIPEDA and should be subject to meaningful and appropriate financial penalties.*

There may be instances where an organization fails to notify individuals whose personal information is at risk as a result of a security breach. Some organizations may notify in an incomplete, ineffective or delayed manner. Tough penalties and enforcement thereof would help to ensure that organizations err on the side of disclosure and notification. For these reasons, there should be significant penalties for failure to notify where clearly required under the Act or where ordered by the Privacy Commissioner.

Appendix: Security Breach Notification Laws (as of Dec.31, 2006)

Canadian Statutes

Reference
Ontario, *Personal Health Information Protection Act*, S.O. 2004, c. 3, Sch. A (PHIPA): online < http://www.e-laws.gov.on.ca/DBLaws/Statutes/English/04p03_e.htm >.

American Federal Statutes

Reference
Gramm-Leach-Bliley Act: online <http://www.ftc.gov/privacy/privacyinitiatives/glbact.html >; and Department of the Treasury, Federal Reserve System, Federal Deposit Insurance Corporation, *Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice*, effective March 29, 2005, online: <http://www.fdic.gov/news/news/financial/2005/fil2705a.pdf>.

American Federal Bills

Reference
Data Accountability and Trust Act (DATA), Bill H.R. 4127: online <http://www.govtrack.us/data/us/bills.text/109/h/h4127.pdf>.
Financial Data Protection Act of 2006, Bill H.R. 3997: online <http://www.govtrack.us/data/us/bills.text/109/h/h3997.pdf>.
Identity Theft Protection Act, Bill S. 1408: online <http://www.govtrack.us/data/us/bills.text/109/s/s1408.pdf>.
Personal Data Privacy and Security Act of 2005, Bill S.1789: online <http://www.govtrack.us/data/us/bills.text/109/s/s1789.pdf>.

American State Statutes

State	Statute
Arizona	S.B. 1338, online: Arizona State Legislature <http://www.azleg.gov/legtext/47leg/2r/bills/sb1338h.pdf>.
Arkansas	S.B. 1167, online: Arkansas 86th General Assembly <http://www.arkleg.state.ar.us/ftproot/bills/2005/public/SB1167.pdf>.
California	S.B. 1386, online: Official California Legislative Information <http://info.sen.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020926_chaptered.html >.
Colorado	H.B. 1119, online: colorado.gov <http://www.state.co.us/gov_dir/leg_dir/olls/sl2006a/sl_145.htm>.
Connecticut	S.B. 650, online: Connecticut General Assembly

	<http://www.cga.ct.gov/2005/act/Pa/2005PA-00148-R00SB-00650-PA.htm>.
Delaware	H.B. 116, online: Delaware General Assembly <http://www.legis.state.de.us/LIS/lis143.nsf/vwLegislation/HB+116/$file/legis.html?open >.
Florida	*An Act relating to unlawful use of personal identification information*, online: Florida House of Representatives <http://www.myfloridahouse.gov/Sections/Documents/loaddoc.aspx?FileName=_h0481er.doc&DocumentType=Bill&BillNumber=0481&Session=2005 >.
Georgia	S.B. 230, online: Georgia General Assembly <http://www.legis.ga.gov/legis/2005_06/fulltext/sb230.htm >.
Hawaii	Security Breach Notification Act of 2006, online: Hawaii State Legislature <http://www.capitol.hawaii.gov/session2006/Bills/SB2290_.htm>.
Idaho	Idaho Code ss.28-51-104 to 28-51-107, online: Idaho State Legislature <http://www3.state.id.us/oasis/2006/S1374.html#daily>.
Illinois	*Personal Information Protection Act*, online: Illinois General Assembly <http://www.ilga.gov/legislation/publicacts/fulltext.asp?Name=094-0036>.
Indiana	Indiana Code § 24-4.9, online: Indiana General Assembly <http://www.in.gov/legislative/ic/code/title24/ar4.9/ >.
Kansas	S.B. 196, online: Kansas Legislature <http://www.kslegislature.org/bills/2006/196.pdf>.
Louisiana	Database Security Breach Notification Law, online: Louisiana State Legislature <http://www.legis.state.la.us/billdata/streamdocument.asp?did=317617>.
Maine	The Notice of Risk to Personal Data Act, online: Maine State Legislature <http://janus.state.me.us/legis/LawMakerWeb/summary.asp?ID=280017964>
Minnesota	H.F. No. 2121, online: Minnesota House of Representatives <http://www.revisor.leg.state.mn.us/bin/bldbill.php?bill=H2121.3&session=ls84>.
Montana	H.B. 732, online: Montana Legislative Branch Website <http://data.opi.state.mt.us/bills/2005/BillPdf/HB0732.pdf >.
Nebraska	L.B. 876, online: Nebraska Legislature <http://www.unicam.state.ne.us/legal/SLIP_LB876.pdf>.
Nevada	S.B. 347, online: Nevada Legislature <http://www.leg.state.nv.us/73rd/bills/SB/SB347_EN.pdf >.
New Hampshire	H.B. 1660, online: New Hampshire House of Representatives <http://www.gencourt.state.nh.us/legislation/2006/HB1660.html>.
New Jersey	*Identity Theft Prevention Act*, online: New Jersey Legislature <http://www.njleg.state.nj.us/2004/Bills/PL05/226_.HTM >.
New York	*Information Security Breach and Notification Act* <http://www.cscic.state.ny.us/lib/laws/documents/899-aa.pdf >.
North Carolina	*Identity Theft Protection Act*, online: North Carolina General Assembly <http://www.ncga.state.nc.us/Sessions/2005/Bills/Senate/HTML/S1048v6.html>.
North Dakota	S.B. 2251, online: North Dakota Legislative Assembly

	<http://www.legis.nd.gov/assembly/59-2005/bill-text/FRBS0500.pdf>.
Ohio	H.B. 104, online: 127th Ohio General Assembly <http://www.legislature.state.oh.us/bills.cfm?ID=126_HB_104>.
Oklahoma	H.B. 2357, online: Oklahoma Legislature <http://webserver1.lsb.state.ok.us/2005-06bills/HB/hb2357_engr.rtf>.
Pennsylvania	*Breach of Personal Information Notification Act*, online: The Pennsylvania General Assembly <http://www2.legis.state.pa.us/WU01/LI/BI/BT/2005/0/SB0712P1410.pdf>.
Rhode Island	*Rhode Island Identity Theft Protection Act of 2005*, online: The State of Rhode Island General Assembly <http://www.rilin.state.ri.us/Billtext/BillText05/HouseText05/H6191.pdf>.
Tennessee	Public Acts, Chapter 473, online: Tennessee General Assembly <http://tennessee.gov/sos/acts/104/pub/pc0473.pdf >.
Texas	*Identity Theft Enforcement and Protection Act*, online: Texas Legislature <http://www.capitol.state.tx.us/tlodocs/79R/billtext/html/SB00122F.htm>.
Utah	*Consumer Credit Proteciton Act*, online: Utah State Legislature <http://www.le.state.ut.us/~2006/bills/sbillenr/sb0069.htm>.
Vermont	S. 284, online: The Vermont Legislature <http://www.leg.state.vt.us/docs/legdoc.cfm?URL=/docs/2006/acts/ACT162.HTM>.
Washington	S.B. 6043, online: Washington State Legislature <http://www.leg.wa.gov/pub/billinfo/2005-06/Htm/Bills/Senate%20Bills/6043-S.htm>.
Wisconsin	S.B. 164, online: Wisconsin State Legislature <http://www.legis.state.wi.us/2005/data/SB-164.pdf>.