Senate Counsel, Research, and Fiscal Analysis

G-17 STATE CAPITOL
75 REV. DR. MARTIN LUTHER KING, JR. BLVD.
ST. PAUL, MN 55155-1606
(651) 296-4791
FAX: (651) 296-7747
JO ANNE ZOFF SELLNER
DIRECTOR

Senate

State of Minnesota

S.F. No. 794 - Membership Travel Contracts

Author: Senator Chris Gerlach

Prepared by: Matthew S. Grosser, Senate Research (651/296-1890)

Date: March 29, 2005

The bill amends Minnesota consumer protection laws regulating membership travel contracts to provide consumers with a right of cancellation up to midnight of the tenth day after the date of consummation, herein defined as the day the consumer has been provided with all materials explaining their rights, obligations, benefits, and restrictions, and all materials necessary to make travel arrangements, under the membership. The bill also requires written notice of the right to cancel prior to extending additional contract offerings, and requires disclosure of certain conditions, requirements, and/or restrictions associated with any gift offering.

MSG:cs

Senators Gerlach and Wiger introduced--

S.F. No. 794: Referred to the Committee on Commerce.

A bill for an act

relating to consumer protection; regulating membership travel contracts; amending Minnesota Statutes 2004, sections 325G.50; 325G.505, subdivision 3; 325G.51; proposing coding for new law in Minnesota Statutes, chapter 325G.

BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF MINNESOTA:

Section 1. Minnesota Statutes 2004, section 325G.50, is amended to read:

325G.50 [MEMBERSHIP TRAVEL CONTRACTS; CANCELLATION.]

Subdivision 1. [DEFINITIONS.] For purposes of this section and ~~section~~ sections 325G.501 and 325G.505, the following terms have the meanings given them:

(a) "Membership travel contract" or "contract" means an agreement offered or sold in this state evidencing a buyer's right to make travel arrangements from or through a membership travel operator and includes a membership that provides for this use.

(b) "Membership travel operator" means a person offering or selling membership travel contracts paid for by a fee or periodic payments.

(c) "Travel arrangements" means travel reservations or accommodations, tickets for domestic or foreign travel by air, rail, ship, bus, or other medium of transportation, or hotel or other lodging accommodations for members.

(d) "Date of consummation of service" means the date on

which the buyer of the contract is provided with all materials necessary to allow the buyer to make travel arrangements that are the subject of the contract and is provided all materials explaining the buyer's rights, obligations, benefits, and restrictions under the membership travel contract.

(e) "Gift" means a prize, award, rebate, bonus, coupon, credit, voucher, or other item of value offered or provided to a consumer as part of the solicitation to purchase a membership travel contract.

Subd. 2. [BUYER'S RIGHT TO CANCEL.] In addition to other rights the buyer may have, the buyer may cancel a membership travel contract until midnight of the tenth business day after the ~~day on which the contract was signed by the buyer~~ date of consummation of service for the contract.

To be effective, a notice of cancellation must be given by the buyer in writing to the membership travel operator at the operator's address. This address must be included in the membership travel contract. The notice, if given by mail, is effective upon deposit in a mailbox, properly addressed to the operator and postage prepaid. The notice is sufficient if it shows, by any form of written expression, the buyer's intention not to be bound by the membership travel contract.

Cancellation is without liability on the part of the buyer and the buyer is entitled to a refund, within ten days after notice of cancellation is given, of the entire consideration paid for the contract. Rights of cancellation may not be waived or otherwise surrendered.

Subd. 3. [WRITTEN NOTICE TO MEMBERS.] A copy of the contract must be delivered to the buyer at the time the contract is signed. The contract must be in writing, must be signed by the buyer, must designate the date on which the buyer signed the contract, and must state, clearly and conspicuously, in boldface type of a minimum size of 14 points immediately adjacent to the buyer's signature, the following:

"MEMBERS' RIGHT TO CANCEL

If you wish to cancel this contract, you may cancel by

delivering or mailing a written notice to the membership travel operator. The notice must say that you do not wish to be bound by the contract and must be delivered or mailed before midnight of the tenth business day after you sign this contract. The notice must be delivered or mailed to: (Insert name and mailing address of membership travel operator). If you cancel, the membership travel operator will return, within ten days of the date on which you give notice of cancellation, any payments you have made. Your right to cancel continues until midnight of the tenth business day after the day on which you are provided with all materials necessary to allow you to make travel arrangements and all materials that explain your rights, obligations, benefits, and restrictions under the contract."

Subd. 3a. [ORAL NOTICE TO MEMBERS.] At the time the contract is signed by the buyer, the membership travel operator shall orally inform the buyer of the buyer's right to cancel the contract ~~within ten business days of the contract signing~~ described in subdivision 2.

Subd. 4. [CANCELLATION AT ANY TIME.] (a) A contract which does not contain the notice specified in subdivision 3 may be canceled by the buyer at any time by giving notice of cancellation by any means.

(b) If the oral notice required by subdivision 3a has not been given to the buyer at the time the contract was signed, the buyer may cancel the contract at any time by giving notice of cancellation by any means.

(c) If the buyer has a continuing right to cancel under this subdivision, the membership travel operator, or any affiliate or successor to the membership travel operator, shall not solicit the buyer to enter into a new contract, unless before the solicitation, the membership travel operator provides the following:

(1) at the same time as the initial written solicitation to enter a new contract, a written notice on a separate sheet of paper that in boldface type of a minimum size of 14 points states the following:

"RIGHT TO CANCEL

You have the right to cancel the contract that you previously entered with (name of membership travel operator). If you cancel the contract with (name of membership travel operator), you have the right to receive a refund of all money paid for the contract. You also will not be required to make any further payments under that contract.

This is an attempt to solicit you to enter a new contract.

If you would like more information concerning Minnesota laws governing membership travel contracts, please contact the Minnesota Attorney General's Office at (the Minnesota Attorney General's Office address and telephone number)."; and

(2) at the same time as the initial oral solicitation to enter a new contract, an oral notice that clearly reiterates the statement contained in clause (1).

The attorney general shall provide a number for insertion into this notice on request of the membership travel operator.

Sec. 2. [325G.501] [MEMBERSHIP TRAVEL CONTRACTS SOLICITATION GIFT OFFERS.]

(a) No membership travel operator shall offer a gift, either directly or indirectly, to a person in Minnesota unless the membership travel operator clearly discloses the following information at the same time and in the same manner and prominence as the offer of the gift:

(1) the true name or names of the travel club operator and the address of the travel club operator's principal place of business;

(2) the estimated retail value of the gift, which must not be more than twice the direct cost to the membership travel operator for the gift;

(3) any requirement that the person receiving the notice pay taxes, refundable or nonrefundable deposits, or any other charges to obtain or use a gift, including the nature and amount of the charges;

(4) if receipt of the gift is subject to a requirement that the person attend a meeting with the travel club operator for

the purpose of soliciting the person to enter into a membership travel contract, a statement that the requirement applies, a description of the membership travel contract the membership travel operator wishes to sell, the approximate length of the meeting, and the requested price for the membership travel contract;

(5) any limitations on eligibility to receive the gift; and

(6) if use of the gift is subject to any restrictions, including, but not limited to, travel restrictions, a statement that a restriction applies, and a detailed description of the restriction.

Sec. 3. Minnesota Statutes 2004, section 325G.505, subdivision 3, is amended to read:

Subd. 3. [ORAL DISCLOSURES.] A membership travel operator shall orally disclose to any prospective purchaser, before a membership travel contract is executed by the prospective purchaser, the information in the public offering statement as required in subdivision 2, ~~clauses (1), (2), and (3),~~ and whether the membership travel operator uses a third-party travel agent or membership travel operator to make travel arrangements provided for in the contract.

Sec. 4. Minnesota Statutes 2004, section 325G.51, is amended to read:

325G.51 [PENALTIES; REMEDIES.]

A person who violates ~~section~~ sections 325G.50 ~~or~~ to 325G.505 is subject to the penalties and remedies provided in section 8.31. The relief provided in this subdivision is in addition to remedies or penalties otherwise provided by law.

Senator Scheid from the Committee on Commerce, to which was referred

S.F. No. 794: A bill for an act relating to consumer protection; regulating membership travel contracts; amending Minnesota Statutes 2004, sections 325G.50; 325G.505, subdivision 3; 325G.51; proposing coding for new law in Minnesota Statutes, chapter 325G.

Reports the same back with the recommendation that the bill do pass and be re-referred to the Committee on Judiciary. Report adopted.

.....
(Committee Chair)

March 30, 2005.....
(Date of Committee recommendation)

Senate Counsel, Research, and Fiscal Analysis

G-17 STATE CAPITOL
75 REV. DR. MARTIN LUTHER KING, JR. BLVD.
ST. PAUL, MN 55155-1606
(651) 296-4791
FAX: (651) 296-7747
JO ANNE ZOFF SELLNER
DIRECTOR

Senate

State of Minnesota

S.F. No. 1379 - Air Bag Repair or Replacement

Author: Senator Linda Scheid

Prepared by: Matthew S. Grosser, Senate Research (651/296-1890)

Date: March 29, 2005

The bill excludes the costs of repairing or replacing deployed air bags and related components in determining whether a vehicle has sustained collision damage totaling more than 70 percent of the retail value of the vehicle prior to the collision. Such a valuation of collision damage is the threshold in Minnesota statute which requires disclosure for title and sale, and the issuance of a salvage title.

MSG:cs

Senators Scheid, Sparks, Marko, Ourada and Murphy introduced--
S.F. No. 1379: Referred to the Committee on Commerce.

A bill for an act

relating to motor vehicles; excluding cost of air bag repair or replacement and related repair costs from motor vehicle damage calculations for salvage title and consumer disclosure purposes; amending Minnesota Statutes 2004, sections 168A.04, subdivision 4; 168A.151, subdivision 1; 325F.6641, subdivisions 1, 2.

BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF MINNESOTA:

Section 1. Minnesota Statutes 2004, section 168A.04, subdivision 4, is amended to read:

Subd. 4. [VEHICLE LAST REGISTERED OUT OF STATE.] If the application refers to a vehicle last previously registered in another state or country, the application shall contain or be accompanied by:

(1) any certificate of title issued by the other state or country;

(2) any other information and documents the department reasonably requires to establish the ownership of the vehicle and the existence or nonexistence and priority of any security interest in it;

(3) the certificate of a person authorized by the department that the identifying number of the vehicle has been inspected and found to conform to the description given in the application, or any other proof of the identity of the vehicle the department reasonably requires; and

(4) with respect to vehicles subject to section 325F.6641,

whether the vehicle sustained damage by collision or other occurrence which exceeded 70 percent of actual cash value. Damage, for the purpose of this calculation, does not include the cost to repair, replace, or reinstall inflatable safety restraints and other vehicle components that must be replaced due to the deployment of the inflatable safety restraints.

Sec. 2. Minnesota Statutes 2004, section 168A.151, subdivision 1, is amended to read:

Subdivision 1. [SALVAGE TITLES.] (a) When an insurer, licensed to conduct business in Minnesota, acquires ownership of a late-model or high-value vehicle through payment of damages, the insurer shall immediately apply for a salvage certificate of title or shall stamp the existing certificate of title with the legend "SALVAGE CERTIFICATE OF TITLE" in a manner prescribed by the department. Within 48 hours of taking possession of a vehicle through payment of damages, an insurer must notify the department in a manner prescribed by the department.

(b) Any person who acquires a damaged motor vehicle with an out-of-state title and the cost of repairs exceeds the value of the damaged vehicle or a motor vehicle with an out-of-state salvage title or certificate, as proof of ownership, shall immediately apply for a salvage certificate of title. A self-insured owner of a late-model or high-value vehicle who sustains damage by collision or other occurrence which exceeds 70 percent of its actual cash value shall immediately apply for a salvage certificate of title. Damage, for the purpose of this calculation, does not include the cost to repair, replace, or reinstall inflatable safety restraints and other vehicle components that must be replaced due to the deployment of the inflatable safety restraints.

Sec. 3. Minnesota Statutes 2004, section 325F.6641, subdivision 1, is amended to read:

Subdivision 1. [DAMAGE.] (a) If a motor vehicle has sustained damage by collision or other occurrence which exceeds 70 percent of its actual cash value immediately prior to

sustaining damage, the seller must disclose that fact to the buyer, if the seller has actual knowledge of the damage. The amount of damage is determined by the retail cost of repairing the vehicle based on a complete written retail repair estimate or invoice, exclusive of the cost to repair, replace, or reinstall inflatable safety restraints and other vehicle components that must be replaced due to the deployment of the inflatable safety restraints.

(b) The disclosure required under this subdivision must be made in writing on the application for title and registration or other transfer document, in a manner prescribed by the registrar of motor vehicles. The registrar shall revise the certificate of title form, including the assignment by seller (transferor) and reassignment by licensed dealer sections of the form, the separate application for title forms, and other transfer documents to accommodate this disclosure. If the seller is a motor vehicle dealer licensed pursuant to section 168.27, the disclosure required by this section must be made orally by the dealer to the prospective buyer in the course of the sales presentation.

(c) Upon transfer and application for title to a vehicle covered by this subdivision, the registrar shall record the term "rebuilt" on the first Minnesota certificate of title and all subsequent Minnesota certificates of title used for that vehicle.

Sec. 4. Minnesota Statutes 2004, section 325F.6641, subdivision 2, is amended to read:

Subd. 2. [FORM OF DISCLOSURE.] The disclosure required in this section must be made in substantially the following form: "To the best of my knowledge, this vehicle has ..... has not ..... sustained damage, exclusive of any costs to repair, replace, or reinstall air bags and other components that were replaced due to deployment of air bags, in excess of 70 percent actual cash value."

Adopted. 3-30-05

03/29/05 [COUNSEL] CBS SCS1379A-1

Senator Scheid moves to amend S.F. No. 1379 as follows:

Page 2, lines 4 and 28, delete "cost" and insert "actual cost incurred"

Page 3, line 5, delete "cost" and insert "actual cost incurred"

Senator Scheid from the Committee on Commerce, to which was referred

S.F. No. 1379: A bill for an act relating to motor vehicles; excluding cost of air bag repair or replacement and related repair costs from motor vehicle damage calculations for salvage title and consumer disclosure purposes; amending Minnesota Statutes 2004, sections 168A.04, subdivision 4; 168A.151, subdivision 1; 325F.6641, subdivisions 1, 2.

Reports the same back with the recommendation that the bill be amended as follows:

Page 2, lines 4 and 28, delete "cost" and insert "actual cost incurred"

Page 3, line 5, delete "cost" and insert "actual cost incurred"

And when so amended the bill do pass and be re-referred to the Committee on Transportation. Amendments adopted. Report adopted.

Linda Scheid

(Committee Chair)

March 30, 2005

(Date of Committee recommendation)

Senate Counsel, Research, and Fiscal Analysis

G-17 STATE CAPITOL
75 REV. DR. MARTIN LUTHER KING, JR. BLVD.
ST. PAUL, MN 55155-1606
(651) 296-4791
FAX: (651) 296-7747
JO ANNE ZOFF SELLNER
DIRECTOR

Senate
State of Minnesota

S.F. No. 1307 - Consumer Security Breach

Author: Senator Satveer Chaudhary

Prepared by: Christopher B. Stang, Senate Counsel (651/296-0539)

Date: March 28, 2005

Section 1 establishes notice procedures for businesses involved in security breaches related to customer information.

Subdivision 1 provides definitions for purposes of the bill.

Subdivision 2 requires any person that conducts business in Minnesota and that owns or licenses computerized data that includes personal information to disclose any breach of the security of the system following discovery of the breach to any resident of Minnesota whose unencrypted personal information was acquired by an unauthorized person. The disclosure must be made in an expedient manner.

Subdivision 3 requires a business that maintains computerized data that includes personal information that the business does not own to notify the owner or licensee of the information of any breaches of the security of the data immediately following discovery if the information was, or is reasonably believed to have been, acquired by an unauthorized person.

Subdivision 4 provides that the notification required may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. In that case, the notification must be made after the law enforcement agency determines that it will not compromise the investigation.

Subdivision 5 specifies methods of notice for purposes of the bill.

Subdivision 6 provides alternative compliance authority for businesses that maintain their own notification procedures as part of an information security policy.

CBS:cs

968

Senators Chaudhary, Skoglund, Sparks, Betzold and Scheid introduced--

S.F. No. 1307: Referred to the Committee on Commerce.

A bill for an act

relating to consumer protection; requiring disclosure to consumers of a breach in security by businesses maintaining personal information in electronic form; proposing coding for new law in Minnesota Statutes, chapter 325G.

BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF MINNESOTA:

Section 1. [325G.48] [BUSINESS MAINTAINING COMPUTERIZED DATA THAT INCLUDES PERSONAL INFORMATION; DISCLOSURE OF BREACH IN SECURITY.]

Subdivision 1. [DEFINITIONS.] For purposes of this section, the terms defined in this subdivision have the meanings given them.

(a) "Breach of the security of the system" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business. Good faith acquisition of personal information by an employee or agent of the person or business for the purposes of the person or business is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure.

(b) "Personal information" means 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:

(1) Social Security number;

(2) driver's license number or Minnesota identification card number; or

(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.

Personal information does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

Subd. 2. [NOTICE TO CONSUMERS.] Any person or business that conducts business in Minnesota, and 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 Minnesota whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure must be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision 4, or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

Subd. 3. [NOTICE TO OWNER OR LICENSEE OF PERSONAL INFORMATION.]

Any person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

Subd. 4. [DELAYED NOTICE.] The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification required by this section must

be made after the law enforcement agency determines that it will not compromise the investigation.

Subd. 5. [METHOD OF NOTICE.] Notice under this section may be provided by one of the following methods:

(1) written notice;

(2) electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in United States Code, title 15, section 7001;

(3) substitute notice, if the person or business demonstrates that the cost of providing notice would exceed $250,000, or that the affected class of subject persons to be notified exceeds 500,000, or the person or business does not have sufficient contact information. Substitute notice consists of all of the following:

(i) e-mail notice when the person or business has an e-mail address for the subject persons;

(ii) conspicuous posting of the notice on the Web site page of the person or business, if the person or business maintains one; and

(iii) notification to major statewide media.

Subd. 6. [ALTERNATE COMPLIANCE.] Notwithstanding subdivision 5, a person or business that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this section, is considered to be in compliance with the notification requirements of this section if the person or business notifies subject persons in accordance with its policies in the event of a breach of security of the system.

Information Security Expert Witnesses in Favor of SF1307

1. Brad Bolin, 651 407 5271
2. Bruce Schneier, 612-823-1098
3. John Weaver, 612.719.2663

Brad Bolin, Practice Manager for Shavlik Technologies,
Attorney-at-law, CISSP*, BS7799 Lead Auditor

Brad is a leading exponent of systematized, standards-based information security management programs, designed to help companies meet security and compliance issues in an efficient, cost-effective manner. He has assisted multiple organizations with developing information security programs that are compliant with major information security-related laws and regulations. Examples include the development of incident response programs designed to handle the exposure of consumer information protected by laws such as GLBA and SB 1386, and security management programs for financial services firms that address the requirements of SOX, GLBA and other relevant legislation.

As a licensed attorney, Brad is uniquely positioned to advise corporations on strategic risk management issues, such as the implications of contemporary data security laws and regulations. As a Certified Information Systems Security Professional ("CISSP") with over 6 years of experience in network and security administration, including risk assessment and mitigation at a number of Minnesota's largest companies, Brad possesses a wide variety of technical skills upon which to draw.

He has recently served as the core information security advisor to the American Bar Association's Information Security Liability and Risk Management Working Group. The goal of the Working Group is to study the impacts of legislation upon the management of information security.

Bruce Schneier
Founder and Chief Technical Officer of Counterpane Internet Security

Internationally-renowned security technologist and author Bruce Schneier is both a Founder and the Chief Technical Officer of Counterpane Internet Security, Inc. the world's leading protector of networked information - the inventor of outsourced security monitoring and the foremost authority on effective mitigation of emerging IT threats.

Schneier is responsible for maintaining Counterpane's technical lead in world-class information security technology and its practical and effective implementation. Schneier's security experience makes him uniquely qualified to shape the direction of the company's research endeavors, as well as to act as a spokesperson to the business community on security issues and solutions.

Schneier is the author of eight books, including his current best seller, *Beyond Fear: Thinking Sensibly about Security in an Uncertain World*, which tackles the problems of security from the small to the large: personal safety, crime, corporate security, national security. *Secrets & Lies: Digital Security in a Networked World*, which was published in October 2000, has sold 100,000 copies. One of his earlier books, *Applied Cryptography*, now in its second edition, is the seminal work in its field and has sold over 150,000 copies and has been translated into five languages. He writes the free email newsletter Crypto-Gram, which has over 100,000 readers. He has presented papers at many international conferences, and he is a frequent writer, contributing editor, and lecturer on the topics of cryptography, computer security, and privacy. Schneier designed the popular Blowfish and Twofish encryption algorithms, the atter a finalist for the new Federal Advanced Encryption Standard (AES). Schneier served on the board of directors of the

---

* NOTES: CISSP – Certified Information System Security Professional, CISA – Certified Information Systems Auditor, CISM – Certified Information Systems Manager, BS7799 – The most widely-recognized international standard for information systems security, scheduled to be adopted by the International Standards Organization. CPP – Certified Protection Professional.

International Association for Cryptologic Research, and is an Advisory Board member for the Electronic Privacy Information Center.

Schneier holds an MS degree in computer science from American University and a BS degree in physics from the University of Rochester.

John Weaver, Information Security Consultant,
CISSP, CISA, CPP, CISM

He has over fifteen years of experience in Internet and Information Security. He directed Information Security of a global IP network providing security architecture, policy, regulatory compliance, operational processes and security metrics for both public and internal networks. He has provided security consulting to Fortune 1000 and International companies in Energy, Telecommunications, Financial and Healthcare vertical markets. He has trained Law Enforcement on Internet security related to criminal investigators. He is a member of the FBI's Minnesota chapter of InfraGard. He is a sought-after speaker and frequent media resource on issue of Internet and Information Security, Cyberterrorism, regulatory compliance and protection of the National Infrastructure.

Statement on SF1307 Minnesota Privacy Notification Act
by Bruce Schneier

The reports of privacy violations are coming in torrents. Criminals are known to have downloaded the personal credit information of over 145,000 Americans from ChoicePoint's network. Hackers took over one of Lexis Nexis', gaining access to the personal files of 32,000 people. Bank of America Corp. lost computer data tapes that contained personal information on 1.2 million federal employees -- including members of the U.S. Senate. A hacker downloaded the names, Social Security numbers, voicemail messages, SMS messages, and photos of 400 T-Mobile customers, and probably had access to all of their 16.3 million U.S. customers. And in a separate incident, Paris Hilton's phone book and SMS messages were hacked and then distributed on the Internet.

The risks of third-party data are twofold. The first is the privacy risk. And the second is impersonation leading to fraud: what is popularly called "identity theft." Identity theft is the fastest-growing crime in the U.S. A criminal collects enough personal data on someone to impersonate him to banks, credit card companies, and other financial institutions. Then he racks up debt in the person's name, collects the cash, and disappears. The victim – over 300,000 in 2003 alone – is left holding the bag, often having to spend years clearing his name. Total losses: $53 billion. Chance of getting caught: 1 in 700, according to a Gartner survey. (Real numbers are probably worse, because many identity thefts go unreported.)

People have been told to be careful: not to give out personal financial information, to shred their trash, to be careful when doing business on-line. But criminal tactics have evolved, and much of this information is useless. Why steal identities one at a time, when you can steal them by the tens of thousands?

The problem is that security of much of our data is no longer under our control.

This is new. A dozen years ago, if someone wanted to look through your mail, he would have to break into your house. Now he can just break into your ISP. Ten years ago, your voicemail was on an answering machine in your house; now it's on a computer owned by a telephone company. Your financial accounts are on websites protected only by passwords; your credit history is stored – and sold – by companies you don't even know exist. Lists of books you buy, and the books you browse, are stored in the computers of online booksellers. Your affinity card allows your supermarket to know what foods you like. Others now control data that used to be under your direct control.

We have no choice but to trust these companies with our security and privacy, even though they have little incentive to protect them. Neither Choicepoint, Lexis Nexis, Bank of America, nor T-Mobile bears the costs of identity theft or privacy violations. We are not their customers. They have no business relationship with us.

And more importantly, these companies are not charities. They should not be expected to deliberately reduce their corporate profits just because we would like them to. If we want them to take the privacy of our personal data seriously, we need to make it in their best interest to do so.

The only reason we know about most of these incidents at all is a California law mandating public disclosure when certain personal information about California residents is leaked. If you read the public statements from ChoicePoint, they were first only going to inform California residents if their information was stolen. They only agreed to alert residents in other states after public outcry. In fact, ChoicePoint arrived at its 145,000 figure because they didn't look back further than the California law mandated.

A similar Minnesota law would protect Minnesotans. It's good public policy. It's good social policy. And it will work.

JBW Group Inc
information security consulting

PO Box 19373
Minneapolis, MN 55419 USA
+1.612.719.2663
www.jbwgroup.com

Position Paper – Endorsing Senate Bill No. 1307 - Privacy Notification

Privacy, as envisioned by the framers of the United States Constitution does not exist in 21st Century America. In the mid-to-late 1960's, a plan for a central database with information on US citizens was opposed on the grounds that it put too much power of information in the hands of a very few and could easily be subject to abuse. The situation we find ourselves in today is that our personal information is being collected everywhere in our society. Data is gathered in just about every aspect of our daily lives and often little is being done to protect that information.

My local drugstore has a record of my prescriptions and what I'm being treated for, my medical records reside in multiple locations; family physician, specialist clinics, medical plan providers, etc.

Part or all of my financial history is stored in multiple places; credit bureaus, banks, credit card clearinghouses and my spending habits are monitored on a regular basis. My mailing address and phone number is traded, bought and sold at so rapid a rate as to make it impossible to stop the flood of junk mail and solicitation calls.

The local video store tracks what movies I've rented, the pizza shack has my pizza preferences and delivery history. Northwest Airlines maintains a record of my travel. Political candidates, parties and PACs all have information about my past contributions, and political leanings.

The phone company maintains records of calls on my land line and cell phone and the GPS chip in the phone can be used to track the location of the phone and my travels.

My Internet surfing is monitored by websites in order to develop a profile of my on-line activities in order to more effectively sell me something. ISPs and ASP cache web pages explicitly to provide quicker response to their customers but the implicit benefit is the sale of web traffic analysis, of great value to marketers. My email address is harvested, bought and sold resulting in a mailbox flooded with marketing for recreational Viagra, bootleg software and pornography. Googling can often produce interesting results, revealing information that should be protected but because of a cavalier attitude or ineptitude is not.

As a result of outsourcing offshore, much of our personally identifiable information now is accessed from or resides in countries that have no laws protecting privacy. The business reality is that it is in the best interest of these off-shore businesses to act with the necessary due diligence to protect the

PO Box 19373
Minneapolis, MN 55419 USA
+1.612.719.2663
www.jbwgroup.com

information that has been entrusted to them but there is little recourse for the individual if the confidentiality of their personal information is breached.

The horror stories are seemingly endless; Choicepoint had their business process compromised which resulted in the disclosure of personal financial information of 150,000 individuals (probably a lot more). In late February a Bank of America cyber-security breach compromised 1.2 million federal employee credit card accounts. In early March a Lexus-Nexus security breach resulted in disclosure of names, addresses, social security numbers, driver's licenses of 32,000 US citizens. DSW Shoe Warehouse suffered a breach of security that resulted in the compromise of shopping habits and credit cards numbers of thousands customers of more than 100 stores. Until recently it has been common practice for the state Departments of Motor Vehicles to sell driver's license information of its citizens. The Kentucky Health Cabinet recycled computer systems that contained the names and contact information of 10,000 AIDS patients in the state. A ring of Eastern European criminals bought and sold valid credit card numbers stolen from e-commerce web sites. And loan and credit applications were discovered in bundles of paper at a Wisconsin recycling facility.

I support Senate Bill 1307 as a necessary first step to raise awareness of the erosion of individual privacy and impose responsibility on those collecting data on behalf of those whose data is being collected.

Next steps for ensuring the privacy of the citizens of Minnesota should include;

- Institute a broader definition of what information should be protected (not just name and account information)
- Expand the definition to include information in all forms beyond digital to include paper, digital in transit and at rest, microfiche, video, audio and spoken words.
- Identify the organizations responsible for enforcement and set penalties for violations
- Provide for full and comprehensible explanation of how information will be used at the point it is being gathered (opt-in)
- Require notification to individuals for the purpose of obtaining approval (or not) before personal information is shared (e.g. selling of lists)
- Provide fair compensation for victims of compromised privacy to include recovery of actual losses
- Enact measures to prevent nuisance civil litigation of privacy violations

PO Box 19373
Minneapolis, MN 55419 USA
+1.612.719.2663
www.jbwgroup.com

John B. Weaver – CISSP, CISA, CISM CPP
President, CEO
JBW Group Inc
International Information Security Consulting

John B. Weaver is British Standards Institute-qualified in BS7799/ISO17799 Information Security Audit and Implementation with over sixteen years experience in Internet and Information Security. He directed Information Security for a global IP network providing security architecture, policy, regulatory compliance, operational processes and security metrics for both public and internal networks. He has provided security consulting to Fortune 1000 and International companies in Energy, Telecommunications, Financial and Healthcare vertical markets. He has trained Law Enforcement on Internet security related to criminal investigations. He is a member of the Federal Bureau of Investigation's Minnesota chapter of InfraGard, serving on the chapter's Executive Board of Directors. He is a sought-after speaker and frequent media resource on issues of Internet and Information Security, Cyberterrorism, regulatory compliance and protection of the National Infrastructure. He has previously spoken before a Minnesota legislative sub-committee on issues of security, privacy and technology.

CALIFORNIA DEPARTMENT OF CONSUMER AFFAIRS

Recommended Practices on Notification of Security Breach Involving Personal Information

October 10, 2003

Joanne McNabb, Chief
Office of Privacy Protection
California Department of Consumer Affairs
www.privacy.ca.gov

Contents

Recommended Practices on Notification of Security Breach

Introduction

The Office of Privacy Protection in the California Department of Consumer Affairs has the statutorily mandated purpose of "protecting the privacy of individuals' personal information in a manner consistent with the California Constitution by identifying consumer problems in the privacy area and facilitating development of fair information practices."[1] Among other things, the law specifically directs the Office to "make recommendations to organizations for privacy policies and practices that promote and protect the interests of California consumers."[2]

In fulfillment of those obligations, the Office of Privacy Protection is publishing these recommended practices for providing notice in cases of security breach involving personal information.

In developing the recommendations, the Office of Privacy Protection received consultation and advice from an advisory group made up of representatives of the financial, health care, retail, technology and information industries; state government agencies; law enforcement; and consumer privacy advocates.[3] The group members' contributions were very helpful and are greatly appreciated.

Identity Theft

We now know that identity theft is much more common than reports in recent years suggested. A national survey conducted by the Federal Trade Commission found that the number of victims in 2002 approached 10 million, and two other recent surveys estimated the number at seven million.[4] That's nearly 10 times greater than the previously quoted estimate of less than a million a year. If the same rate is applied to California, then over a million Californians became victims of identity theft in the past year.

The surveys also confirmed the opinions of law enforcement and others that identity theft is on the rise in the U.S., showing a dramatic increase between 2001 and 2002.[5]

The costs of the crime are alarming. Recent studies estimate the average victim's out-of-pocket expenses at $500 to $740, and the time spent clearing up the situation at from 30 to several hundred hours.[6] The Federal Trade Commission estimates the total annual cost to business as $50 billion for 2002, based on an average loss from the misuse of a victim's personal information of $4,800.[7]

Studies also show that the cost of an identity theft incident, both for victims and for business, is significantly lower if it is discovered quickly.[8]

Security Breaches

Security is an essential component of information privacy. It is one of the basic principles of fair information practice: Organizations that collect or manage individuals' personal information should use security safeguards to protect that information against unauthorized access, use, disclosure, modification or destruction.[9] Implementing an effective information security program is essential for an organization to fulfill its responsibility towards the individuals who entrust it with their personal information. It is the best way to reduce the risk of exposing individuals to the possibility of identity theft. It is also the best way to reduce the risk of exposing the organization to the cost of an information security breach to its reputation and finances.

Most business and all government agencies today acknowledge their responsibility for ensuring the security of the personal information in their care. In its 2000 report to Congress on the privacy practices of companies doing business online, the Federal Trade Commission found that the privacy policies of 74 percent of the 100 most popular Web sites included a statement that they took steps to provide security for the information they collected.[10] Many

organizations in the U.S. are legally required to protect the security of personal information. The two major federal laws on privacy enacted in recent years—the Gramm-Leach-Bliley Act and the Health Information Portability and Accountability Act—include security rules that apply to a broad range of financial institutions and health care organizations.[11] The California Information Practices Act requires government agencies to establish safeguards to ensure the security and confidentiality of records.[12]

Nevertheless, information security studies have indicated that the number of breaches has increased over time, along with their frequency, severity and the costs to business of responding.[13] One recent survey found that 39 percent of the large global financial institutions responding acknowledged that their systems had been compromised in the past year, although the researcher commented that the figure seemed low compared to other surveys showing that nearly 80 to 90 percent of Fortune 500 companies and government agencies have experienced breaches.[14]

California, which leads the nation in privacy protection statutes, has recently enacted a law to address this situation. The law is intended to give individuals early warning when their personal information has fallen into the hands of an unauthorized person, so that they can take steps to protect themselves against identity theft or to mitigate the crime's impact.

In order to get an early look at how a number of major corporations had prepared to implement the new California law on notification of security breach, the Ponemon Institute conducted a preliminary benchmark survey in early July 2003, as the law first took effect.[15] The study suggests that corporations have been prompted to take action by the law, including acquiring enabling technologies to protect their information technology infrastructure from data breaches, and that the law does not create a significant cost-of-compliance burden. The study also revealed some areas where best practice guidance was sought, such as encryption and coordination of notification responsibilities of third parties with whom data is shared.

California Law on Notification of Security Breach

California Civil Code Sections 1798.29 and 1798.82 to 1798.84 apply to any person or business in California and to government agencies. The full text of the law is attached as Appendix 3. The main provisions are summarized below.

Security Breach

- Unauthorized acquisition of computerized data the compromises the security, confidentiality or integrity of personal information.

Type of Information

- Unencrypted computerized data including certain personal information.
- Personal information that triggers the notice requirement is name (first name or initial and last name) plus any of the following:
  - Social Security number,
  - Driver's License or California Identification Card number, OR
  - Financial account number, credit or debit card number (along with any PIN or other access code where required for access to account).

Whom to Notify

- Notice must be given to any data subjects who are California residents.

When to Notify

- Timing: "in the most expedient time possible and without unreasonable delay." Time may be allowed for the following:
  - Legitimate needs of law enforcement if notification would impede a criminal investigation
  - Taking necessary measures to determine the scope of the breach and restore reasonable integrity to the system.

How to Notify

- Notice may be provided in writing, electronically (as consistent with provisions on electronic records and signatures per 15 USC 7001), or by substitute notice.
- Substitute notice may be used if the cost of providing individual notice is >$250,000 or if >500,000 people would have to be notified. Substitute notice means all of the following:
  - E-mail when the e-mail address is available, and
  - Conspicuous posting on agency web site, and
  - Notification of major statewide media.
- Alternatively, the business or agency may use its own notification procedures as part of an information security policy for personal information, if its procedures are consistent with the timing requirements of the law and if it notifies subjects in accordance with its policy.

Recommended Practices

The Office of Privacy Protection's recommendations are intended to assist organizations in supplementing their information security programs. The recommendations are not regulations and are not binding. Nor are they limited to the scope of the California law on notice of security breach, but rather they represent a broader approach and a higher standard.

These "best practices" recommendations can serve as guidelines for organizations, to assist them in providing timely and helpful information to individuals whose personal information has been compromised while in the organization's care. Unlike many best practices sets, however, these recommendations do not contain all the practices that should be observed. Information-handling practices and technology are changing rapidly, and organizations should continuously review and update their own situation to ensure compliance with the laws and principles of privacy protection. It is recognized that specific or unique considerations, including compliance with other laws, may make some of these practices inappropriate for some organizations.

Our practice recommendations are presented in three parts: Part 1 - Protection and Prevention, Part II - Preparation for Notification, and Part III - Notification. While the California law on notice of security breach applies only to records in electronic media ("computerized data") and defines a limited set of items of personal information as triggering the notification requirement, we recommend applying these practices to records in any media, including paper records.

Definitions

The following are the definitions of key terms used in these recommended practices.

Notice-triggering information: As provided in California law, this is unencrypted, computerized first name or initial and last name plus any of the following: Social Security number, driver's license number, California Identification Card number, or financial account number, credit or debit card number, in combination with any code or password permitting access to an individual's financial account where such a code or password is required.

Higher-risk personal information: Not only the notice-triggering information that could subject an individual to identity theft, but also health information, other financial information and other personal information the disclosure of which would violate the privacy of individuals.

Data owner: The individual or organization with primary responsibility for determining the purpose and function of a record system.

Data custodian: The individual or organization that has responsibility delegated by the data owner for maintenance and technological management of the record system.

Part 1: Protection and Prevention

While an organization's information security program may be unique to its situation, there are recognized basic components of a comprehensive, multi-layered program to protect personal information from unauthorized access.[16] An organization should protect the confidentiality of personal information whether it pertains to customers, employees or others. For both paper and electronic records, these components include physical, technical and administrative safeguards. Among such safeguards are the following recommended practices.

1. Collect the minimum amount of personal information necessary to accomplish your business purposes, and retain it for the minimum time necessary.
2. Inventory records systems, critical computing systems and storage media to identity those containing personal information.
    - Include laptops and handheld devices used to store personal information.

3. Classify personal information in records systems according to senstivity.
   - Identify notice-triggering information.
4. Use physical and technological security safeguards as appropriate to protect personal information, particularly higher-risk information such as Social Security number, driver's license number, California Identification Card number, financial account numbers and any associated passwords and PIN numbers, other financial information, and health information, in paper as well as electronic records.
   - Authorize employees to have access to only the specific categories of personal information their job responsibilities require.
   - Where possible, use technological means to restrict internal access to specific categories of personal information.
   - Monitor employee access to higher-risk personal information.
   - Remove access privileges of former employees and contractors immediately.
5. Promote awareness of security and privacy policies and procedures through ongoing employee training and communications.
   - Monitor employee compliance with security and privacy policies and procedures.
   - Include all new, temporary, and contract employees in security and privacy training and monitoring.
   - Impose penalties for violation of security and privacy policies and procedures.
6. Require third-party service providers and business partners who handle personal information on behalf of your organization to follow your security policies and procedures.
   - Make privacy and security obligations of third parties enforceable by contract.
   - Monitor and enforce third-party compliance with your privacy and security policies and procedures.
7. Use intrusion detection technology and procedures to ensure rapid detection of unauthorized access to higher-risk personal information.
   - Conduct periodic penetration tests to determine effectiveness of systems and staff procedures in detecting and responding to security breaches.
8. Wherever feasible, use data encryption, in combination with host protection and access control, to protect higher-risk personal information.
   - Data encryption should meet the National Institute of Standards and Technology's Advanced Encryption Standard.[17]
9. Dispose of records and equipment containing personal information in a secure manner, such as shredding paper records with a cross-cut shredder and using a program to "wipe" and overwrite the data on hard drives.[18]
10. Review your security plan at least annually or whenever there is a material change in business practices that may reasonably implicate the security of personal information. For example, if an organization decides to outsource functions that use personal information, such as using a call center, the plans should be revisited to take the new third parties into account.

Part II: Preparation for Notification

An information security program should include an incident response plan, which addresses security incidents including unauthorized access to or acquisition of higher-risk personal information.[19] To ensure timely notice to affected individuals when appropriate, the following practices are among those that should be included in an incident response plan:

1. Adopt written procedures for internal notification of security incidents that may involve unauthorized access to higher-risk personal information.
2. Designate one individual as responsible for coordinating your internal notification procedures.
3. Regularly train employees, including all new, temporary and contract employees, in their roles and responsibilities in your incident response plan.
    - Collect 24/7 contact numbers for incident response team and provide to team members.
4. Define key terms in your incident response plan and identity responsible individuals.
5. Plan for and use measures to contain, control and correct any security incident that may involve higher-risk personal information.
6. Require the data custodian or others who detect an information security incident to immediately notify the data owner upon the detection of any security incident that may involve unauthorized access to the record system.
7. Require third-party service providers and business partners to adopt and follow your security incident notification procedures.
    - Monitor and contractually enforce third party compliance with your security incident response procedures.
8. Identify appropriate law enforcement contacts to notify on security incidents that may involve illegal activities. Appropriate law enforcement agencies include California's regional high-tech crimes task forces, the Federal Bureau of Investigation, the U.S. Secret Service, the National Infrastructure Protection Center, and the local police or sheriff's department. See Appendix 4, page 27, for contact information.
9. Consider suggestions from law enforcement with expertise in investigating high-technology crimes for inclusion in your incident response plan.[21]
10. Be sure to collect contact information (mailing address and/or e-mail address) from individuals whose notice-triggering personal information you collect or manage.
    - If you plan to contact affected individuals by e-mail, get the individuals' prior consent to the use of e-mail for that purpose, as provided in the federal Electronic Signature Act.[22]
11. Adopt written procedures for notification of individuals whose unencrypted notice-triggering personal information has been, or is reasonably believed to have been, acquired by an unauthorized person.
    - Include unauthorized acquisition of computer printouts and other paper records containing notice-triggering personal information in your notification procedures.
12. Document response actions taken on an incident. This will be useful to your organization and to law enforcement, if involved.
    - At the conclusion of an incident, review events and actions and make any indicated changes in your technology and response plan.
13. Review incident response plan at least annually or whenever there is a material change in your business practices that may reasonably implicate the security of personal information.

Part III: Notification

Openness or transparency is another basic privacy principle. An organization that collects or manages personal information should be open about its information policies and practices.[23] This responsibility includes informing individuals about incidents such as security breaches that have caused their unencrypted personal information to be acquired by unauthorized persons. The purpose of notifying individuals of such incidents is to enable them to take actions to protect themselves against, or mitigate the damage from, identity theft or other possible harm.

To ensure giving timely and helpful notice to affected individuals, the following practices are recommended.

Acquisition: In determining whether unencrypted notice-triggering information has been *acquired*, or is reasonably believed to have been acquired, by an unauthorized person, consider the following factors, among others:

1. Indications that the information is *in the physical possession and control* of an unauthorized person, such as a lost or stolen computer or other device containing unencrypted notice-triggering information.
2. Indications that the information has been *downloaded* or copied.
3. Indications that the information was *used* by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported.

Timing of Notification: Notify affected individuals in the most expedient time possible after the discovery of an incident involving unauthorized access to notice-triggering information.

1. Take necessary steps to contain and control the systems affected by the breach and conduct a preliminary internal assessment of the scope of the breach.
2. Once you have determined that the information was, or is reasonably believed to have been, acquired by an unauthorized person, notify affected individuals within 10 business days. Do this unless law enforcement authorities tell you that providing notice at that time would impede their investigation.

Contacting Law Enforcement: If you believe that the incident may involve illegal activities, report it to appropriate law enforcement agencies.[24]

1. In contacting law enforcement, inform the law enforcement official in charge of the investigation that you intend to notify affected individuals within 10 business days as above.
2. If the law enforcement official in charge tells you that giving notice within that time period would impede the criminal investigation:
   - Ask the official to inform you as soon as you can notify the affected individuals without impeding the criminal investigation.
   - It should not be necessary for a law enforcement agency to complete an investigation before notification can be given.
   - Be prepared to send the notices immediately upon being so informed.

Whom to Notify: If your assessment leads you to reasonably believe that notice-triggering information was acquired by an unauthorized person, implement your notification plan.

1. Notify California residents whose notice-triggering information was acquired by an unauthorized person.
2. Notify affected individuals in situations involving unauthorized acquisition of notice-triggering information in any format, including computer printouts and other paper records.
3. Consider providing notice in breaches involving higher-risk personal information, even when it is not "notice-triggering" information under California law, if being notified would allow individuals to take action to protect themselves from possible harm.
4. If you cannot identify the specific individuals whose notice-triggering information was acquired, notify all those in the groups likely to

have been affected, such as all whose information is stored in the files involved.

5. Avoid false positives. A false positive occurs when the required notice of a security breach is sent to individuals who should not receive it because their personal information was not acquired as part of the breach. Consider the following when identifying the group that will be notified:
   - Before sending individual notices, make reasonable efforts to include only those individuals whose notice-triggering information was acquired.
   - Implement procedures for determining who gets included in the notice and who does not. Check the mailing list before sending the notice to be sure it is not over-inclusive.
   - Document your process for determining inclusion in the group to be notified.

Coordination with Credit Reporting Agencies: Consumer credit reporting agencies (Equifax, Experian, and TransUnion) can help you give affected individuals information on the best ways for them to contact the agencies. A breach involving a large number of individuals can potentially have a significant impact on consumer reporting agencies and their ability to respond efficiently. High volumes of calls could impede access to the agencies. Be sure to contact the agencies before you send out notices in cases involving a large number of individuals—10,000 or more.

1. Make arrangements with the credit reporting agencies during your preparations for giving notice, without delaying the notice for this reason.
2. Organizations should contact the consumer credit reporting agencies as follows.
   - **Experian**: E-mail to BusinessRecordsVictimAssistance@experian.com.
   - **Equifax**: Chris Jarrard, Vice President - US Customer Services, Equifax Information Services, LLC, Phone: 678-795-7090, E-mail: chris.jarrard@equifax.com.
   - **TransUnion**: E-mail to fvad@transunion.com, with "Database Compromise" as subject.

Contents of Notice: Sample notice letters are attached as Appendix 2. Include the following information in your notice to affected individuals:

1. A general description of what happened.
2. The nature of the individual's personal information that was involved (not the Social Security number or other actual items of information).
3. What you have done to protect the individual's personal information from further unauthorized acquisition.
4. What your organization will do to assist individuals, including providing an internal contact telephone number, preferably toll-free, for more information and assistance.
5. Information on what individuals can do to protect themselves from identity theft, including contact information for the three credit reporting agencies.
6. Contact information for the California Office of Privacy Protection and/or the Federal Trade Commission for additional information on protection against identity theft.
   - California Office of Privacy Protection
     866-785-9663
     www.privacy.ca.gov
   - Federal Trade Commission
     877-ID-THEFT/877-438-4338
     www.consumer.gov/idtheft/

Form and Style of Notice: Make the notice clear, conspicuous and helpful.

1. Use clear, simple language, guiding subheads, and plenty of white space in the layout.
2. Avoid jargon or technical language.
3. Avoid using a standardized format, which could result in making the public complacent about the process and thus undercut the purpose of the notice.

4. To avoid confusion, the notice should be a stand-alone document, not combined as part of another mailing.

Means of Notification: Individual notice to those affected is preferable whenever possible.

1. Send the notice to all affected individuals by first class mail.
2. Or notify by e-mail, if you normally communicate with the affected individuals by e-mail and you have received the prior consent of the individuals to that form of notification.
3. If more than 500,000 individuals were affected or if the cost of giving individual notice to affected individuals is greater than $250,000 and you are using the "substitute notice" procedures:
   - Send the notice by e-mail to all affected parties whose e-mail address you have; AND
   - Post the notice conspicuously on your web site; AND
   - Notify major statewide media (television, radio, print).

End Notes

[1] California Business & Professions Code section 350(a).
[2] California Business & Professions Code section 350(c).
[3] A list of the members of the advisory group is attached as Appendix 1.
[4] The Federal Trade Commission (FTC)'s, *Identity Theft Survey Report* of September 2003, estimated that 4.6% of American adults were victims in 2002, is available at <http://www.ftc.gov/os/2003/09/synovatereport.pdf>. The two other surveys, released in July 2003, were conducted by Harris Interactive for Privacy and American Business (P&AB) and by Gartner Inc. The P&AB/Harris survey report is available at <http://www.pandab.org> and the Gartner survey report at <http://www3.gartner.com/Init>.
[5] The FTC survey put the increase at 41%, while P&AB/Harris and Gartner both found an 80% increase from 2001 to 2002.
[6] The FTC's report estimated the average out-of-pocket cost to victims at $500, while the P&AB/Harris study put the average cost at $740. The FTC estimated average time spent by victims at 30 hours. A California study by the Identity Theft Resource Center (ITRC), "Identity Theft: The Aftermath 2003," found much higher costs in time and money. The ITRC estimated that the average victim spent nearly $1,500 on such items as telephone calls, postage, mileage, time lost from work, legal assistance, child care, translation costs, notarizing documents, and court fees. The ITRC report also found that the average victim spent 600 hours clearing up the consequences of the crime. The ITRC surveyed victims who had contacted the organization for assistance and who may have been experiencing more serious problems than those of the randomly sampled victims in the FTC's study. The ITRC report is available at <www.idtheftcenter.org>.
[7] The Identity Theft Resource Center estimated the cost to business as much higher, in excess of $279 billion, based on average loss per victim of more than $92,000. The ITRC says that the difference may be explained by the fact that their interviewers were experienced identity theft assistants who spent more time with each respondent than the survey company used by the FTC.
[8] See FTC, *Identity Theft Survey Report* (September 2003), pages 6-8.
[9] This formulation of the security safeguards principle is from the Organisation for Economic Cooperation and Development (OECD)'s *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, available at <http://www1.oecd.org/publications/e-book/9302011E.PDF>.
[10] FTC, *Privacy Online: Fair Information Practices in the Electronic Marketplace*, available at <http://www.ftc.gov/reports/privacy2000/privacy2000.pdf>.
[11] The Gramm-Leach-Bliley Act, 15 USC 6801-6827, includes the Safeguards Rule, "Standards for Insuring the Security, Confidentiality, Integrity and Protection of Customer Records and Information," 16 C.F.R. Part 314. The Health Insurance Portability and Accountability Act, PL 104-191, includes "Health Insurance Reform: Security Standards," 45 C.F.R. Parts 160, 162, and 164.
[12] California Civil Code Section 1798.21. The Information Practices Act, Civil Code Section 1798 et seq., imposes several specific responsibilities for protecting the security and confidentiality of records containing personal information.
[13] See, for example, the CSI/FBI Computer Crime and Security Survey (2002 and 2003), available at <www.gocsi.com>.
[14] Gerry Fitzpatrick of Deloitte & Touche, quoted in *The Register,* May 15, 2003. Deloitte's *2003 Global Security Survey* is available at < www.deloitte.com/gfsi >,
[15] A report on the Ponemon Benchmark Study on Corporate Compliance with California Law on Public Notification of Security Breach is attached as Appendix 6.
[16] The internationally recognized information security standard is ISO/IEC 17799, a comprehensive set of controls comprising best practices in information security. For more information on the principles and practices of information security, see Appendix 5: Information Security Resources.
[17] Effective May 26, 2002, the encryption standard approved for U.S Government organizations and others to protect higher-risk information is FIPS 197. For more information, see Appendix 5.
[18] Standards for "clearing and sanitizing" equipment of data are in the U.S. Department of Defense's National Industrial Security Program Operating Manual, DoD 5220.22M, Chapter 8.306, available at <http://www.defenselink.mil/nii/org/sio/ia/diap/documents/ASD_HD_Disposition_memo060401.pdf>.

[19] ISO/IEC 17799, cited in note 16 above, includes practices relating to responding to and reporting security incidents and malfunctions "as quickly as possible" (§ 6.3).
[20] See Appendix 4 for suggestions on computer security incident response from the California Highway Patrol's Information Management Division.
[21] 15 U.S.C. Section 7001 contains the requirements for consumer disclosure and consent to electronic notification, as required by California Civil Code Sections 1798.29(g)(2) and 1798.82(g)(2).
[22] See the OECD's *Guidelines*, cited in note 8.
[23] See Appendix 4 for definition of "computer crime" in California Penal Code Section 502(c) and suggestions on information to provide to law enforcement.

Appendix 1: Advisory Group List

Advisory Group to Office of Privacy Protection on Recommended Practices on Notice of Security Breach

Brent Barnhart
Senior Counsel
Kaiser Foundation Health Plan, Inc.

Camille Busette
Senior Policy Manager
Intuit

Dianne Carpenter
Senior Attorney
J.C. Penney Corporation
California Retailers Association

James Clark
California Bankers Association

Mari Frank
Attorney, Privacy Consultant and Author

Beth Givens
Director
Privacy Rights Clearinghouse

Roxanne Gould
Vice President, CA Public and Legislative Affairs
American Electronics Association

Chief Kevin Green
California Highway Patrol

Craig Grivette
Deputy Secretary for Business
Enterprise Technology
Business, Transportation and Housing Agency

Tony Hadley
Experian

Gail Hillebrand
Senior Attorney
Consumers Union

Clark Kelso
State Chief Information Officer

Barbara Lawler
Chief Privacy Officer
Hewlett-Packard

Fran Maier
Executive Director
TRUSTe

Dana Mitchell
Counsel to Rules Committee
California State Senate

Peter Neumann
Principal Scientist
Computer Science Lab
SRI International

Dr. Larry Ponemon
Ponemon Institute

Debra Reiger
State Information Security Officer
California Department of Finance

Tim Shea
Legal Counsel
California Franchise Tax Board

Scott Shipman
Privacy Counsel
eBay

Preston Taylor
Consultant to Assemblyman Simitian
California State Assembly

Tracey Thomas
Identity Theft Resource Center

Tom Timmons
President & CEO, Spectrum Bank
President, CA Independent Bankers

Appendix 2: Sample Notice Letters

SAMPLE LETTER 1
Data Acquired: Credit card Number or Financial Account Number

Dear :

I am writing to you because a recent incident may have exposed you to identity theft.

[*Describe what happened in general terms, what kind of personal information was involved, and what you are doing in response.*]

[*Name of your organization*] is writing to you so that you can take steps to protect yourself from the possibility of identity theft. We recommend that you immediately contact [*credit card or financial account issuer*] at [*phone number*] and close your account. Tell them that your account may have been compromised. If you want to open a new account, ask [*name of account issuer*] to give you a PIN or password. This will help control access to the account

To further protect yourself, we recommend that you place a fraud alert on your credit file. A fraud alert lets creditors know to contact you before opening new accounts. Just call any one of the three credit reporting agencies at the number below. This will let you automatically place fraud alerts and order your credit report from all three.

Equifax	Experian	Trans Union
800-525-6285	888-397-3742	800-680-7289

When you receive your credit reports, look them over carefully. Look for accounts you did not open. Look for inquiries from creditors that you did not initiate. And look for personal information, such as home address and Social Security number, that is not accurate. If you see anything you do not understand, call the credit agency at the telephone number on the report.

If you do find suspicious activity on your credit reports, call your local police or sheriff's office and file a report of identity theft. [*Or, if appropriate, give contact number for law enforcement agency investigating the incident for you.*] Get a copy of the police report. You may need to give copies to creditors to clear up your records.

Even if you do not find any signs of fraud on your reports, the California Office of Privacy Protection recommends that you check your credit reports every three months for the next year. Just call one of the numbers above to order your reports and keep the fraud alert in place.

For more information on identity theft, we suggest that you contact the Office of Privacy Protection. The toll-free number is 866-785-9663. Or you can visit their web site at www.privacy.ca.gov. If there is anything [*name of your organization*] can do to assist you, please call [*phone number, toll-free if possible*].

[*Closing*]

SAMPLE LETTER 2
(Data Acquired: Driver's License or California ID Card Number)

Dear :

I am writing to you because a recent incident may have exposed you to identity theft.

[*Describe what happened in general terms, what kind of personal information was involved, and what you are doing in response.*]

[*Name of your organization*] is writing to you so that you can take steps to protect yourself from the possibility of identity theft. Since your Driver's License [*or California Identification Card*] number was involved, we recommend that you immediately contact your local DMV office to report the theft. Ask them to put a fraud alert on your license. This will cut off government access to your license record. Then call the toll-free DMV Fraud Hotline at 866-658-5758 for additional information.

To further protect yourself, we recommend that you place a fraud alert on your credit file. A fraud alert lets creditors know to contact you before opening new accounts. Just call any one of the three credit reporting agencies at the number below. This will let you automatically place fraud alerts and order your credit report from all three.

Equifax	Experian	Trans Union
800-525-6285	888-397-3742	800-680-7289

When you receive your credit reports, look them over carefully. Look for accounts you did not open. Look for inquiries from creditors that you did not initiate. And look for personal information, such as home address and Social Security number, that is not accurate. If you see anything you do not understand, call the credit agency at the telephone number on the report.

If you do find suspicious activity on your credit reports, call your local police or sheriff's office and file a report of identity theft. [*Or, if appropriate, give contact number for law enforcement agency investigating the incident for you.*] Get a copy of the police report. You may need to give copies to creditors to clear up your records.

Even if you do not find any signs of fraud on your reports, the California Office of Privacy Protection recommends that you check your credit reports every three months for the next year. Just call one of the numbers above to order your reports and keep the fraud alert in place.

For more information on identity theft, we suggest that you contact the Office of Privacy Protection. The toll-free number is 866-785-9663. Or you can visit their web site at www.privacy.ca.gov. If there is anything [*name of your organization*] can do to assist you, please call [*phone number, toll-free if possible*].

[*Closing*]

SAMPLE LETTER 3
(Data Acquired: Social Security Number)

Dear :

I am writing to you because a recent incident may have exposed you to identity theft.

[*Describe what happened in general terms, what kind of personal information was involved, and what you are doing in response.*]

[*Name of your organization*] is writing to you so that you can take steps to protect yourself from the possibility of identity theft.

We recommend that you place a fraud alert on your credit file. A fraud alert lets creditors know to contact you before opening new accounts. Then call any one of the three credit reporting agencies at the number below. This will let you automatically place fraud alerts and order your credit report from all three.

Equifax	Experian	Trans Union
800-525-6285	888-397-3742	800-680-7289

When you receive your credit reports, look them over carefully. Look for accounts you did not open. Look for inquiries from creditors that you did not initiate. And look for personal information, such as home address and Social Security number, that is not accurate. If you see anything you do not understand, call the credit agency at the telephone number on the report.

If you do find suspicious activity on your credit reports, call your local police or sheriff's office and file a police report of identity theft. [*Or, if appropriate, give contact number for law enforcement agency investigating the incident for you.]* Get a copy of the police report. You may need to give copies of the police report to creditors to clear up your records.

Even if you do not find any signs of fraud on your reports, the California Office of Privacy Protection recommends that you check your credit report every three months for the next year. Just call one of the numbers above to order your reports and keep the fraud alert in place.

For more information on identity theft we sugest that you contact the Office of Privacy Protection. The toll-free numbers is 866-785-9663. Or you can visit their web site at www.privacy.ca.gov. If there is anything [*name of your organization*] can do to assist you, please call [*phone number, toll-free if possible*].

[*Closing*]

Appendix 3: California Law on Notice of Security Breach

California Civil Code

1798.29. (a) 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. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision (c), or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

(b) Any agency that maintains computerized data that includes personal information that the agency does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

(c) The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification required by this section shall be made after the law enforcement agency determines that it will not compromise the investigation.

(d) For purposes of this section, "breach of the security of the system" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the agency. 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.

(e) For purposes of this section, "personal information" means 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:

(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.

(f) For purposes of this section, "personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

(g) For purposes of this section, "notice" may be provided by one of the following methods:

(1) Written notice.
(2) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in Section 7001 of Title 15 of the United States Code.
(3) Substitute notice, if the agency demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars ($250,000), or that the affected class of subject persons to be notified

exceeds 500,000, or the agency does not have sufficient contact information. Substitute notice shall consist of all of the following:

(A) E-mail notice when the agency has an e-mail address for the subject persons.
(B) Conspicuous posting of the notice on the agency's Web site page, if the agency maintains one.
(C) Notification to major statewide media. (h) Notwithstanding subdivision (g), an agency that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this part shall be deemed to be in compliance with the notification requirements of this section if it notifies subject persons in accordance with its policies in the event of a breach of security of the system.

1798.82. (a) Any person or business that conducts business in California, and 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. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision (c), or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

(b) Any person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

(c) The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification required by this section shall be made after the law enforcement agency determines that it will not compromise the investigation.

(d) For purposes of this section, "breach of the security of the system" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business. Good faith acquisition of personal information by an employee or agent of the person or business for the purposes of the person or business is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure.

(e) For purposes of this section, "personal information" means 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:

(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.

(f) For purposes of this section, "personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

(g) For purposes of this section, "notice" may be provided by one of the following methods:

(1) Written notice.
(2) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in Section 7001 of Title 15 of the United States Code.
(3) Substitute notice, if the person or business demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars ($250,000), or that the affected class of subject persons to be notified exceeds 500,000, or the person or business does not have sufficient contact information. Substitute notice shall consist of all of the following:

(A) E-mail notice when the person or business has an e-mail address for the subject persons.
(B) Conspicuous posting of the notice on the Web site page of the person or business, if the person or business maintains one.
(C) Notification to major statewide media.

(h) Notwithstanding subdivision (g), a person or business that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this part, shall be deemed to be in compliance with the notification requirements of this section if the person or business notifies subject persons in accordance with its policies in the event of a breach of security of the system.

1798.83. Any waiver of the provisions of this title is contrary to public policy, and is void and unenforceable.

1798.84. (a) Any customer injured by a violation of this title may institute a civil action to recover damages.
(b) Any business that violates, proposes to violate, or has violated this title may be enjoined.
(c) The rights and remedies available under this section are cumulative to each other and to any other rights and remedies available under law.

Appendix 4: Reporting Computer Crimes to Law Enforcement

Law Enforcement Contacts for Computer Crimes

California High Technology Theft and Apprehension Program

This program funds five regional task forces staffed by investigators from local, state and federal law enforcement agencies who have received specialized training in the investigation of high technology crime and identity theft investigations. High technology crimes are those crimes in which technology is used as an instrument in committing, or assisting in the commission of, a crime, or is the target of a criminal act.

Sacramento Valley Hi-Tech Crimes Task Force
Telephone: 916-874-3002
www.sachitechcops.org

Southern California High Tech Task Force
Telephone: 562-345-4260

Northern California Computer Crimes Task Force
Telephone: 707-253-4500
www.nc3tf.org

Rapid Enforcement Allied Computer Team (REACT)
Telephone: 408-494-7186
http://reacttf.org

Computer and Technology Crime High-Tech Response Team (CATCH)
Telephone: 619-531-36601
http://www.catchteam.org/

FBI

Local Office: http://www.fbi.gov/contact/fo/fo.htm

National Computer Crime Squad
Telephone: 202-324-9161
E-mail: nccs@fbi.gov
http://www.emergency.com/fbi-nccs.htm

NIPC

National Infrastructure Protection Center
U.S. Department of Homeland Security
Online Reporting: http://www.nipc.gov/incident/incident.htm
Telephone: 202-323-3205
Toll-Free Telephone:888-585-9078
E-mail: nipc.watch@fbi.gov

U.S. Secret Service

Local Office: http://www.treas.gov/usss/index.shtml

Reporting a Computer Crime to Law Enforcement

Guidance from the California Highway Patrol Information Management Division

When reporting a computer crime be prepared to provide the following information:

- Name and address of the reporting agency.
- Name, address, e-mail address, and phone number(s) of the reporting person.
- Name, address, e-mail address, and phone number(s) of the Information Security Officer (ISO).
- Name, address, e-mail address, and phone number(s) of the alternate contact (e.g., alternate ISO, system administrator, etc.)
- Description of the incident.
- Date and time the incident occurred.
- Date and time the incident was discovered.
- Make/model of the affected computer(s).
- IP address of the affected computer(s).
- Assigned name of the affected computer(s).
- Operating System of the affected computer(s).
- Location of the affected computer(s).

Incident Response DOs and DON'Ts

DOs

1. Immediately isolate the affected system to prevent further intrusion, release of data, damage, etc.
2. Use the telephone to communicate. Attackers may be capable of monitoring E-mail traffic.
3. Immediately notify an appropriate law enforcement agency.
4. Activate all auditing software, if not already activated.
5. Preserve all pertinent system logs, e.g., firewall, router, and intrusion detection system.
6. Make backup copies of damaged or altered files, and keep these backups in a secure location.
7. Identify where the affected system resides within the network topology.
8. Identify all systems and agencies that connect to the affected system.

9. Identify the programs and processes that operate on the affected system(s), the impact of the disruption, and the maximum allowable outage time.

10. In the event the affected system is collected as evidence, make arrangements to provide for the continuity of services, i.e., prepare redundant system and obtain data back-ups. To assist with your operational recovery of the affected system(s), pre-identify the associated IP address, MAC address, Switch Port location, ports and services required, physical location of system(s), the OS, OS version, patch history, safe shut down process, and system administrator or backup.

DON'Ts

1. Don't delete, move, or alter files on the affected systems.

2. Don't contact the suspected perpetrator.

3. Don't conduct a forensic analysis.

California Penal Code Definition of "Computer Crime"[1]

As defined by California Penal Code Section 502, subsection (c), a computer crime occurs when a person:

(1) Knowingly accesses and without permission alters, damages, deletes, destroys, or otherwise uses any data, computer, computer system, or computer network in order to either (A) devise or execute any scheme or artifice to defraud, deceive, or extort, or (B) wrongfully control or obtain money, property, or data.

(2) Knowingly accesses and without permission takes, copies, or makes use of any data from a computer, computer system, or computer network, or takes or copies any supporting documentation, whether existing or residing internal or external to a computer, computer system, or computer network.

(3) Knowingly and without permission uses or causes to be used computer services.

(4) Knowingly accesses and without permission adds, alters, damages, deletes, or destroys any data, computer software, or computer programs which reside or exist internal or external to a computer, computer system, or computer network.

(5) Knowingly and without permission disrupts or causes the disruption of computer services or denies or causes the denial of computer services to an authorized user of a computer, computer system, or computer network.

(6) Knowingly and without permission provides or assists in providing a means of accessing a computer, computer system, or computer network in violation of this section.

(7) Knowingly and without permission accesses or causes to be accessed any computer, computer system, or computer network.

(8) Knowingly introduces any computer contaminant into any computer, computer system, or computer network.

(9) Knowingly and without permission uses the Internet domain name of another individual, corporation, or entity in connection with the sending of one or more electronic mail messages, and thereby damages or causes damage to a computer, computer system, or computer network.

Notes

[1] Other violations of California or federal law may also be involved in an incident of unauthorized acquisition of personal information. California laws that may be involved include identity theft (Penal Code § 530.5), theft (Penal Code § 484), or forgery (Penal Code § 470).

Appendix 5: Information Security Resources

CERT®, "Security Improvement Modules," available at < http://www.cert.org/security-improvement/index.html#practices >.

Federal Trade Commission, "Financial Institutions and Customer Data: Complying with the Safeguards Rule," available at <http://www.ftc.gov/bcp/conline/pubs/buspubs/safeguards.htm >.

Federal Trade Commission, "Security Check: Reducing Risks to Your Computer Systems," available at < http://www.ftc.gov/bcp/conline/pubs/buspubs/security.htm >.

"Health Insurance Reform: Security Standards; Final Rule," 45 CFR Parts 160, 162 and 164, available at <http://www.cms.hhs.gov/hipaa/hipaa2/regulations/security/default.asp>.

Internet Security Alliance, "Common Sense Guide for Senior Managers: Top Ten Recommended Information Security Practices," (July 2002), available at <http://www.isalliance.org/news/requestform.cfm >.

National Institute for Standards and Technology (NIST) Computer Security Resource Center at <www.csrc.nist.gov>.

State Administrative Manual, Sections 4840-4845: Security and Risk Management, available at < http://sam.dgs.ca.gov/TOC/4800/default.htm >.

Appendix 6: Benchmark Study

2003 Benchmark Study of Corporate Compliance with the New California Law on Notification of Security Breach
Prepared by Dr. Larry Ponemon, August 28, 2003

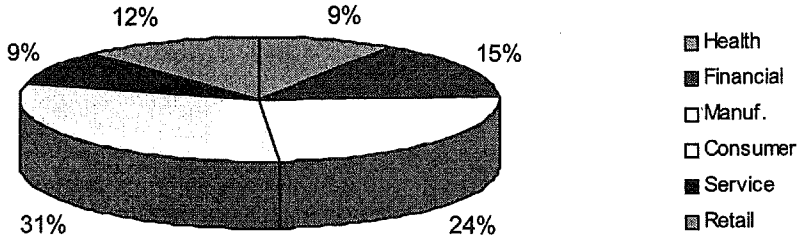
Executive Summary

Ponemon Institute is pleased to present the summary results of a preliminary benchmark study of corporate response to the new California law for notification of data security breaches (effective July 1, 2003). This current study was conducted jointly with sponsorship from Internet Security Solutions (ISS). We anticipate that results from the study will provide a meaningful baseline for measuring and monitoring trends in how leading organizations are responding to new regulatory requirements as required by California state law (civil code sections 1798.29 and 1798.82-1798.84).

The current benchmark study was conducted through confidential interviews using a fixed form design with a representative group of either privacy or information security leaders representing 34 companies. All participating individuals and companies volunteered without compensation. All companies were promised complete anonymity, and no company identification information was collected.

In total, 71 business (and governmental) organizations were contacted in July 2003 by the researcher to enroll participants in this study. The criteria for participation was twofold: (a) applicability of the new California law to the company's current operations and (b) the organizational position of the respondent with respect to domain-specific knowledge about data protection or information security practices within his or her company.

All 35 companies contacted by the researcher agreed to participate in the required timeline. One company was removed from the final analysis based on incomplete responses, resulting in a final study of 34 businesses with the following industry representation.



While most companies were large (Fortune 500 organizations), eight companies were medium sized organizations (less than $1 billion in annual revenues).

The interviewer asked respondents a series of questions from a fixed form instrument to glean information about how organizations were responding to the new California law on notification of a security breach. Information about communication processes, organization structure, enabling

technologies and attitudes about compliance with the new law were asked. Specific drill-down questions about the information security technology to enhance compliance with the notification security breach law were pursued (not reported here).

Based on preliminary findings, many corporations are approaching their compliance with the new California law with only minor or insignificant changes being made to the communication process and technology infrastructure. As noted below, 76% of respondents said that the law motivated their companies to change the process for communicating a data security breach, yet more than 35% view these changes as relatively insignificant or immaterial to the process that was in-place before the law.

While not captured in the Tables below, several respondents mentioned that the proper handling of notice or communications at the time of crisis (such as a security breach of sensitive personal information) is an opportunity to show key stakeholders that the company will do the "right" thing with the data entrusted to them. They also acknowledged that the improper execution of notice would sorely impact the company's brand or image in the marketplace.

A large number of respondents seem to have a compliance mindset when it comes to managing the required notice and communications process. Some feel that the process in-place today is mere form over substance because it does little to protect the customer or employee. Despite a negative view by some, the majority of companies have decided to go beyond required California residents, implementing the revised notification on an enterprise-wide (national or global) basis.

The following tables summarize the main questions and results of our study.

Table 1A shows that the largest segment of participating companies are implementing an enterprise procedure for communicating data security breaches, as opposed to a segmented approach just for California residents.

Table 1A:
The security breach communications process within your company as required by CA law pertains to:

	Freq.	Pct%
California residents	7	21%
All individuals in the U.S.	14	41%
All individuals (global)	4	12%
Not decided as yet	8	24%
No comment	1	3%
Totals:	*34*	*100%*

Table 1B shows that the majority of companies consider all personal information as part of the required notification. This view goes beyond the limited variables cited in the regulation. However, 18% of respondents appear to view the new law as applying to customer or consumer information only (which could be a compliance breach).

Table 1B:
Security breach communications program pertains to:

	Freq.	Pct%
All records about individuals and households	20	59%
All records about individuals	8	24%
Only customers & consumers	4	12%
Only customers	2	6%
Only employees	0	0%
Totals:	*34*	*100%*

Table 2 shows that most companies have changed or updated their process for notice of a security breach as a direct result of the new California law.

Table 2:
Did your company's communication process for data security breaches change as a result of the new law?

	Freq.	Pct%
Yes	26	76%
No	5	15%
Unsure	3	9%
Totals:	*34*	*100%*

In corroboration of the above finding, Table 3 shows that 79% of respondents believe that the new law will increase the need for resources in order to achieve reasonable compliance.

Table 3:
Do the requirements of the CA law require your organization to incur additional resources?

	Freq.	Pct%
Yes	27	79%
No	4	12%
Unsure	3	9%
Totals:	*34*	*100%*

Table 4 shows that more than half consider resource requirements under the new law to be moderate or insignificant. Only 15% of participants view this required increase in resources as significant.

Table 4:
How substantial are resource requirements in order to comply with the new CA law?

	Freq.	Pct%
Significant	5	15%
Moderate	8	24%
Insignificant	12	35%
Unsure	9	26%
Totals:	*34*	*100%*

Items contained within Tables 5A, 5B and 5C show that many participants are still uncertain about the IT infrastructure impact of the California law.

About 32% of respondents believe that perimeter controls (such as firewalls and other devices) have changed (or will soon change) as a result of compliance requirements with the new law.

Table 5A:
Did your company's perimeter control processes change as a result of the new law?

	Freq.	Pct%
Yes	11	32%
No	8	24%
Unsure	15	44%
Totals:	*34*	*100%*

Again, 32% of subjects believe that IDS or related processes have changed (or will soon change) or have been improved as a result of the new California law (Table 5B).

Table 5B:
Did your company's intrusion detection systems (IDS) change as a result of the new law?

	Freq.	Pct%
Yes	11	32%
No	10	29%
Unsure	13	38%
Totals:	*34*	*100%*

More than 41% of respondents believe that the use of encryption technologies changed (or will soon change) as a direct result of new compliance requirements in California.

Table 5C:
Did your company's use of encryption change as a result of the new law?

	Freq.	Pct%
Yes	14	41%
No	15	44%
Unsure	5	15%
Totals:	*34*	*100%*

As noted in Table 6A, the operating structure for managing notice requirements varies among the 34 benchmark companies. While 44% of respondents state that their companies have centralized control of breach communications, more than 21% believe that their companies have either ad hoc control or no clear procedures in place.

Table 6A:
What is the organization structure for ensuring communications for data security breaches are compliant with the new law?

	Freq.	Pct%
Centralized control process in-place	15	44%
Partially centralized control process in-place	7	21%
Decentralized control process in-place	5	15%
Informal (ad hoc) control process in-place	3	9%
No clear control process in-place	4	12%
Totals:	*34*	*100%*

Table 6B shows a large variance in who is in-charge of the notice of security breaches within their organizations today. As can be seen, 24% of respondents state that "no one" is currently responsible for this important function.

Table 6B:
Who is in-charge of the data security breach communication process within your organization?

	Freq.	Pct%
No one	8	24%
IT leader	7	21%
Privacy Officer (or CPO)	6	18%
Security Office (or CISO)	5	15%
General Counsel or associate	4	12%
Chief Information Officer	1	3%
Communications or public affairs	2	6%
Other	1	3%
Totals:	*34*	*100%*

Table 7A shows that 62% have a specified timeline for executing required notice and communications in the case of a security breach defined under California law.

Table 7A:
Does your company have a specific timeline for executing notice to individuals subject to communication under the new law?

	Freq.	Pct%
Yes	21	62%
No	10	29%
Unsure	3	9%
Totals:	*34*	*100%*

For those who answered "yes" to the above question, Table 7B shows that for 71% of respondents the specified time limit is 10 days or less after a known breach has occurred. However, most respondents said this specified time is an internal metric subject to delay based on the investigation and enforcement process.

Table 7B:
Is your company's the timeline for executing notice about a data security breach less than 10 business days?

	Freq.	Pct%
Yes	15	71%
No	6	29%
Unsure	0	0%
Totals:	*21*	*100%*

Table 8 shows that more than 47% of respondents state that the use or collection of SSN or SIN information has changed (or will soon change) as a direct consequence of the new law.

Table 8:
Did your company's use of social security numbers (SSN and SIN) change as a result of the new law?

	Freq.	Pct%
Yes	16	47%
No	14	41%
Unsure	4	12%
Totals:	*34*	*100%*

Table 9 shows that 29% of respondents believe the company's use of encryption is sufficient to warrant safe harbor status under the new law. However, this belief varies considerably based on the technical background of the responding individual. Specifically, individuals with 10 of the 12 "yes" respondents were individuals with non-technical backgrounds (typically a lawyer or compliance officer). In contrast, 9 of the 10 "no" respondents were information security specialists with significant IT background.

Table 9:
Do your current encryption procedures over individual data warrant the safe harbor provision under the new CA law?

	Freq.	Pct%
Yes	10	29%
No	12	35%
Unsure	12	35%
Totals:	*34*	*100%*

The questions in Table 10A and Table 10B focus on data sharing with third parties or affiliates. In general, respondents were uncertain about how their companies manage (or plan to manage) notice about data security breaches resulting from events, errors or abuses caused by an external party such as vendors, outsourced contractors and so forth.

Table 10A shows that 41% of respondents do not plan to expand current compliance requirements for notice of a data security breach to third parties. Another 21% of respondents are uncertain about changing compliance requirements for third parties.

Table 10A:
Does your company's notice of a security breach as required under the new law pertain to exposed data shared with third parties or affiliates?

	Freq.	Pct%
Yes	13	38%
No	14	41%
Unsure	7	21%
Totals:	*34*	*100%*

Table 10B shows that 38% of respondents review (or plan to review) business partners (and other third parties) with respect to their internal compliance procedure for the provision of notice; however, such due diligence procedures appear to be either informal or superficial. Over 32% admit to doing no due diligence for data protection compliance beyond the initial contract phase.

Table 10B:
Do you review (or plan to review) business partners' compliance with the new California law?

	Freq.	Pct%
Yes	13	38%
No	11	32%
Unsure	10	29%
Totals:	*34*	*100%*

Table 11 shows that 32% of companies changed (or plan to change) their confidential communication procedures with law enforcement authorities as a result of the new law in California. However, a large number of respondents (21%) are still uncertain about how law enforcement should be brought into the investigation and enforcement process.

Table 11:
Did the new law change your company's process or procedures for communicating a data security breaches with law enforcement authorities?

	Freq.	Pct%
Yes	11	32%
No	16	47%
Unsure	7	21%
Totals:	*34*	*100%*

Table 12A summarizes the core compliance question for the benchmark sample. As can be seen, 48% of subjects are at least moderately confident that their organizations are in reasonable compliance with the notice requirement. However, 32% are either not confident about compliance or admit to being non-compliant with the law. A large percentage of participants (21%) declined to comment.

Table 12A:
As of today, how confident are you that your company is in reasonable compliance with the law CA law?

	Freq.	Pct%
Very confident	1	3%
Confident	7	21%
Moderately confident	8	24%
Not confident	10	29%
Not in compliance	1	3%
No comment	7	21%
Totals:	*34*	*100%*

Table 12B provides the frequency and percentage for six companies headquartered in California. As can be seen, of the six participants, five are either confident or very confident that their organizations are in reasonable compliance with the new law.

Table 12B:
As of today, how confident are you that your company is in reasonable compliance with the law CA law?

	Freq.	Pct%
Very confident	1	17%
Confident	4	67%
Moderately confident	0	0%
Not confident	1	17%
Not in compliance	0	0%
No comment	0	0%
Totals:	*6*	*100%*

Table 12C provides the frequency and percentage for companies in regulated industries that already require a data security breach communication (i.e., financial services under GLB Safeguards Rule and healthcare under HIPAA). Of the eight regulated companies, seven are at least moderately confident that their organizations are in reasonable compliance with the new law.

Table 12C:
As of today, how confident are you that your company is in reasonable compliance with the law CA law?

	Freq.	Pct%
Very confident	1	13%
Confident	5	63%
Moderately confident	1	13%
Not confident	1	13%
Not in compliance	0	0%
No comment	0	0%
Totals:	*8*	*100%*

Table 13 summarizes respondents' opinions about the law. It is interesting to note that 74% believe the new law in California will be repealed or significantly changed. The main reason for this belief is the apparent cost versus benefits for business and the public.

Table 13:
Do you believe that the new CA law will be repealed or significantly changes over time?

	Freq.	Pct%
Yes	25	74%
No	5	15%
Unsure	4	12%
Totals:	*34*	*100%*

Ponemon Institute
Attn: Research Department
3901 S. Escalante Ridge Place
Tucson, Arizona 85730
520.290.3400
research@ponemon.org

RAY Kaplan & ASSOCIATES
INFORMATION SECURITY & PRIVACY SERVICES

P.O. Box 130039 . St. Paul, MN 55113 . ray@rayk.com . 1+ 651.235.8201

March 30, 2005 Position Statement: SF 1307 Chaudhary Bill
as introduced 84th Legislative Session (2005-2006) and posted on Feb 25, 2005

Thank you for the opportunity to testify about this important legislation.

I have timed my remarks to be a brief summary of my written testimony.

I am Ray Kaplan of Ray Kaplan & Associates. I have been an information systems security consultant for over 20 years and in the computer industry for over 30 years.

While I am quite passionate about the need for this type of legislation, I am opposed to SF 1307 as it is written. I am also opposed to its apparent twin, SF 1805 (Dibble bill.)

I am in agreement with many, if not all, of the suggestions that my colleagues have made. In particular, John Weaver's vision of the future for Minnesota citizen privacy and the views of Robert Aanerud who I believe is being represented here by Rob Ramer in support of SF 1307. I'll go them one better by asserting that Minnesota needs a privacy office similar to the California Department of Consumer Affairs' Office of Privacy Protection (http://www.privacy.ca.gov/lawenforcement/laws.htm)

I find the following serious deficiencies with the current version of SF 1307 and SF 1805:

1. **Both of these bills are apparently merely clones of California SB1386**, which added substantially the same verbiage into Section 1498 of the California State Civil Code in 2002.

   Despite the fact that SB1386 was pace-setting, events have moved past this legislation and I believe that Minnesota needs to seize the high ground by continuing its tradition of leadership in this area by adequately protecting its citizen's privacy. **Simply cloning the California legislation is inadequate.**

2. **There are no sanctions in this bill**

   Organizations are not compelled in any way to comply. At the very least, **sanctions should be imposed that ensure victims can be made whole** in accordance with Constitution of the State of Minnesota (as amended):

   > Sec. 8. Every person is entitled to a certain remedy in the laws for all injuries or wrongs which he may receive to his person, property or character, and to obtain justice freely and without purchase, completely and without denial, promptly and without delay, conformably to the laws.

3. **Subdivision 1 [Definitions]**

Paragraph (a), "Breach of Security" - For clarity, this needs to be defined more carefully to specifically include explanatory phrases in common English such as "unauthorized disclosure" in conjunction with "confidentiality" and "corruption" in conjunction with "integrity." Terms such as "security" need to be more precisely defined and should include terms such as "unauthorized use", "misuse." Organization for Economic Cooperation and Development (OECD) privacy principle 5, Security Safeguards Principle, states: "*Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.*" **The terminology in this bill should be explained and better defined in accordance with International, national, and industry standards; US Federal law; other state laws; and Minnesota Statutes, such as Chapter 13, Government Data Practices.**

Paragraph (b), "Personal Information" – This should be more precisely and more broadly defined. For instance, personal information certainly includes middle names and initials. **This definition should be harmonized with commonly accepted definitions** in International, national, and industry standards; International law, US Federal law; other state laws; and Minnesota Statutes, such as Chapter 13, Government Data Practices sections, including Section 13.02, Collection, security, and dissemination of records; definitions. **The definition should recognize that combinations of personal information whose individual components may be public (such as name, account number, and mother's maiden name) require special protection since those combinations are especially useful to identity thieves.** The definition should include biometrics (picture, signature, finger print…) The fact that personal information can be stored on a variety of media such as paper, electronic database, photographic and video image, digital form and may also extend to body sample and biometric data should be recognized.

Paragraph (b), "Personal Information" – specifically excludes encrypted data elements. This is inappropriate since such encryption may not be done in accordance with commonly accepted best practice. Even when best practices are employed, hard questions remain such as *How long can encrypted data elements that end up in the wrong hands withstand attack by a well-equipped adversary such as well-funded organized crime syndicate that is devoted to identity theft?* **This bill should specify that the methods of protecting personal information that are exempted should be done on accordance with commonly accepted standards and best practices. However, since encrypted information is not immune to compromise, it should not be exempted.**

Paragraph (b), "Personal Information" – specifically excludes publicly available information. This exemption should NOT include non-public

information, such as that that needs to be further defined by this section, that was derived using publicly available information. This may seem like splitting hairs, but suffice it to say that the capabilities of organizations that have access to a wide variety of databases can derive an amazing array of non-public information by using the wide variety of public information that is available to them.

4. **Subdivision 2 [Notice to Consumers]**

   This section, again, exempts encrypted personal information. It should not do so. Encryption is only a useful defense if it is practices in accordance with best practices. Further, many difficult questions must be answered such as *"How long can the encryption protect personal information that ends up in the wrong hands in the face of a dedicated attack by a well-armed adversary such as a well-funded organized crime syndicate that specializes in identity theft?* Encryption is one of the ways that information can be protected. **This bill should specify that the methods of protecting personal information that are exempted should be done on accordance with commonly accepted standards and best practices. However, since encrypted information is not immune to compromise, it should not be exempted.**

5. **Subdivision 3 [Notice To Owner or Licensee Of Personal Information]**

   This Subdivision does not specify any requirement for these "partners" (contractors, service agencies…) to protect the personal information and **it does not specify any sanctions** that the "partner" would suffer as a result of the failure to notify the owner or licensee.

   This Subdivision does not specify that the owner or licensee must, in turn, notify in accordance with Subdivision 2 and **it does not specify any sanctions** for failure to make that notification. **This notification should be required and sanctions for failure should be specified.**

6. **Subdivision 5 [Method of Notice]**

   This subdivision states that notice "may" be provided. It should say "must."

   This Subdivision states that notice may be provided by only one of the methods listed. This is inadequate. Notice should be provided by several of the methods listed. For instance, written notice and conspicuous posting of the notice on the organization's Web site.

   This Subdivision exempts notification where sufficient contact information is not available. This is inappropriate. A good faith effort to obtain sufficient contact information should be required.

Section (3) Substitute Notice states lists several methods of notification as substitutes. These methods of notice should be listed as additional methods of notification that are required. For instance, despite the fact that we have come to rely on it, **e-mail is not a guaranteed or reliable method of message delivery. Having e-mail as a sole substitute for written notice is not reasonable.**

Section (3) Substitute Notice exempts notification efforts that would cost more than $250,000 or involve more than 500,000 notifications. This is inappropriate. While the theft of personal information on 10 people is certainly a problem, the loss of personal information on 1,000,000 people is a huge problem. **Such large amounts of personal information are only useful to well-organized, well-funded syndicates of professional identity thieves.** The relationship between the amount of personal information compromised and the seriousness of the problem is linear: the more personal information that is compromised, the more dangerous the compromise. **This section's ceilings are arbitrary and should be removed.**

7. **Subdivision 6 [Alternative Compliance]**

This Subdivision specifies that an organization may use its own notification procedures so long as they are consistent with the timing requirements of the section. This is inadequate. Such notification procedures **should be consistent with the whole bill and should specifically require the notification method's requirements.**

RAY Kaplan & ASSOCIATES
INFORMATION SECURITY & PRIVACY SERVICES

P.O. Box 130039 . St. Paul, MN 55113 . ray@rayk.com . 1+ 651.235.8201

Ray Kaplan

CISSP, CISSP-ISSAP, ISSMP, CISA, CISM, Qualified BS7799 Auditor and Implementer

Ray Kaplan is a certified information security professional with over 20 years of experience in information security and over 30 years of experience in the computing industry. He is widely known in the security community for the breadth and depth of his expertise and continues to be a prolific public speaker and published author. As a long-time security evangelist, he has given hundreds of presentations all over the world in forums ranging from user groups to conferences, seminars and private venues. He continues to provide security consulting on a broad range of topics and to deliver certification training and technical tutorials along with his participation in many industry forums and consortia. His experience includes the managerial, personnel and technical aspects of information security, including architecture, policy, standards, design, implementation, management and operations. Ray was the recipient of the Computer Security Institute's (CSI) 1999 Lifetime Achievement Award in recognition of his contributions to CSI and the industry.

A Track Record of Contributions

- Assessed infrastructures and information security management systems against applicable laws, regulations, standards and standards of due care
- Writings included in the Common Body of Knowledge on which the Certified Information Systems Security Professional (CISSP) is based
- Taught the 5 day ISC(2) CISSP Common Body of Knowledge seminar
- Serves on the editorial board of the Auerbach Journal on Information Security
- Continues to write for security journals and the security trade press
- Continues to present for domestic and international security conferences
- Consulted with organizations from all segments of the economy including telecommunications, financial, manufacturing, academic and governmental to understand and address their information security and information assurance needs
- Acts as a mentor to less experienced security professionals
- Collaborated with information security consulting organizations and security product vendors to form, improve and maintain their information security practices
- Focused internationally working with clients from Japan, Australia, South Africa, Scandinavia, Europe, the United States and Canada.
- Worked with very small organizations (1 person and 1 network point of presence) to the very large (over 875,000 people and 40,000 network points of presence)

Certifications

- Certified Information Systems Security Professional (CISSP) – 1998; CISSP-ISSMP, ISSAP – 2005
- Certified Information Systems Auditor (CISA) – 2001
- Certified Information Security Manager (CISM) – 2002
- Qualified BS7799 Auditor and Implementer – 2003, 2004
- Certified HIPAA Security Professional (CHSP) – 2002

Professional Affiliations

- Computer Security Institute (CSI) – Member
- Information Systems Security Association (ISSA) – Member
- Information Systems Audit and Control Association (ISACA) – Member
- Institute of Electrical and Electronic Engineers (IEEE) – Member
- The High Tech Crime Investigator's Association (HTCIA) – Member
- Information Systems Forensics Association (ISFA) – Member
- FBI's Critical Infrastructure Protection Program (Infragard) – Member
- Upper Midwest Infragard (Minnesota and Dakotas) – Member of the Executive Board
- UNIX Users Group (USENIX) – Member

SF 1307 Chaudhary Bill

S.F. No. 1307, as introduced 84th Legislative Session (2005-2006) Posted on Feb 25, 2005

A bill for an act

relating to consumer protection; requiring disclosure to consumers of a breach in security by businesses maintaining personal information in electronic form; proposing coding for new law in Minnesota Statutes, chapter 325G.

BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF MINNESOTA:

Section 1. [325G.48] [BUSINESS MAINTAINING COMPUTERIZED DATA THAT INCLUDES PERSONAL INFORMATION; DISCLOSURE OF BREACH IN SECURITY.]

Subdivision 1. [DEFINITIONS.] For purposes of this section, the terms defined in this subdivision have the meanings given them.

(a) "Breach of the security of the system" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business. Good faith acquisition of personal information by an employee or agent of the person or business for the purposes of the person or business is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure.

(b) "Personal information" means 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:

(1) Social Security number;

(2) driver's license number or Minnesota identification card number; or

(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.

Personal information does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

Subd. 2. [NOTICE TO CONSUMERS.] Any person or business that conducts business in Minnesota, and 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 Minnesota whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure must be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision 4, or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

Subd. 3. [NOTICE TO OWNER OR LICENSEE OF PERSONAL INFORMATION.]

Any person or business that maintains computerized data

that includes personal information that the person or business does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

Subd. 4. [DELAYED NOTICE.] The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification required by this section must be made after the law enforcement agency determines that it will not compromise the investigation.

Subd. 5. [METHOD OF NOTICE.] Notice under this section may be provided by one of the following methods:

(1) written notice;

(2) electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in United States Code, title 15, section 7001;

(3) substitute notice, if the person or business demonstrates that the cost of providing notice would exceed $250,000, or that the affected class of subject persons to be notified exceeds 500,000, or the person or business does not have sufficient contact information. Substitute notice consists of all of the following:

(i) e-mail notice when the person or business has an e-mail address for the subject persons;

(ii) conspicuous posting of the notice on the Web site page of the person or business, if the person or business maintains one; and

(iii) notification to major statewide media.

Subd. 6. [ALTERNATE COMPLIANCE.] Notwithstanding subdivision 5, a person or business that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this section, is considered to be in compliance with the notification requirements of this section if the person or business notifies subject persons in accordance with its policies in the event of a breach of security of the system.

Senator Scheid from the Committee on Commerce, to which was referred

S.F. No. 1307: A bill for an act relating to consumer protection; requiring disclosure to consumers of a breach in security by businesses maintaining personal information in electronic form; proposing coding for new law in Minnesota Statutes, chapter 325G.

Reports the same back with the recommendation that the bill do pass and be re-referred to the Committee on Judiciary. Report adopted.

Linda Scheid
(Committee Chair)

March 30, 2005
(Date of Committee recommendation)

Senate Counsel, Research, and Fiscal Analysis

G-17 State Capitol
75 Rev. Dr. Martin Luther King, Jr. Blvd.
St. Paul, MN 55155-1606
(651) 296-4791
FAX: (651) 296-7747
Jo Anne Zoff Sellner
Director

Senate

State of Minnesota

S.F. No. 664 - Omnibus Liquor Bill (Subcommittee Report)

Author: Senator Sandra L. Pappas

Prepared by: Christopher B. Stang, Senate Counsel (651/296-0539)

Date: March 22, 2005

Section 1 (Pappas) would permit brewpubs whose total off-sales in any 12-month period amount to less than ten percent of their total on premises malt beverage production or 100 barrels, whichever is less, to use wort produced outside Minnesota. Current law prohibits brewpubs from using wort produced outside Minnesota.

Section 2 (Pogemiller) allows Minneapolis to issue an on-sale intoxicating liquor license to the Guthrie Theater's concessionaire for a restaurant at the Guthrie Theater.

Section 3 (Ourada) allows a wine tasting to take place for more than four hours duration at a large convention of fine wine and gourmet food exhibitors.

Section 4 (Anderson) requires an authority issuing a retail liquor license or operating a municipal liquor store to impose specified minimum penalties for sales to underage persons. Two annual mandatory compliance checks on each retail license holder or municipal liquor store are also required.

Section 5 (Ourada) allows on-sales of 3.2 malt liquor at 10:00 a.m. on Sundays.

Section 6 (Ourada) allows on-sale of intoxicating liquor at 10:00 a.m. on Sundays without requiring that a municipality hold a public hearing and pass an ordinance.

Section 7 (Ourada) provides for a uniform time statewide of 10:00 p.m. for off-sale of intoxicating liquor on Mondays through Saturdays.

Section 8 (Robling) allows Elko to authorize liquor sales on all days of the week at a restaurant/banquet facility at the Elko Speedway.

Section 9 (Hann) allows Eden Prairie to issue an on-sale intoxicating liquor license to the entity holding an operating food service contract at a cafeteria at a designated building owned by the city.

Section 10 (Hottinger) allows Mankato to issue an on-sale intoxicating liquor license to the Midwest Wireless Civic Center.

Section 11 (Wergin) allows the Mille Lacs County Board to issue an off-sale intoxicating liquor license to a liquor store in Eastside Township, notwithstanding a distance requirement from a city operating a municipal liquor store in Minnesota law.

CBS:cs

To: Senator Scheid, Chair

Committee on Commerce

Senator Pappas,

Chair of the Subcommittee on Liquor, to which was referred

S.F. No. 664: A bill for an act relating to alcoholic beverages; allowing a brewer who manufactures beer on the premises where the brewer also holds an on-sale intoxicating liquor license to use wort produced outside Minnesota under certain circumstances; amending Minnesota Statutes 2004, section 340A.301, subdivision 6.

Reports the same back with the recommendation that the bill be amended as follows:

Delete everything after the enacting clause and insert:

"Section 1. Minnesota Statutes 2004, section 340A.301, subdivision 6, is amended to read:

Subd. 6. [FEES.] The annual fees for licenses under this section are as follows:

(a) Manufacturers (except as provided in clauses (b) and (c))	$15,000
Duplicates	$ 3,000
(b) Manufacturers of wines of not more than 25 percent alcohol by volume	$ 500
(c) Brewers other than those described in clauses (d) and (i)	$ 2,500

(d) Brewers who also hold one or more retail on-sale licenses and who manufacture fewer than 3,500 barrels of malt liquor in a year, at any one licensed premises, using only wort produced in Minnesota <u>except as otherwise provided in this clause</u>, the entire production of which is solely for consumption on tap on the licensed premises or for off-sale from that licensed premises. A brewer licensed under this clause<u>:</u>

<u>(1)</u> must obtain a separate license for each licensed premises where

the brewer brews malt liquor. ~~A brewer licensed under this clause~~; (2) may not be licensed as an importer under this chapter; and (3) may use wort produced outside Minnesota if (i) its total sales at off-sale under section 340A.301, subdivision 7, paragraph (b), in any 12-month period do not exceed ten percent of the total production of beer on the premises or 100 barrels, whichever is less, or (ii) in the case of a brewer who has been licensed under this clause for fewer than 12 months, if the commissioner reasonably determines that the brewer will not sell amounts at off-sale in excess of the amounts specified in item (i) during the first 12 months of licensing $ 500

(e) Wholesalers (except as provided in clauses (f), (g), and (h)) $15,000

Duplicates $ 3,000

(f) Wholesalers of wines of not more than 25 percent alcohol by volume $ 2,000

(g) Wholesalers of intoxicating malt liquor $ 600

Duplicates $ 25

(h) Wholesalers of 3.2 percent malt liquor $ 10

(i) Brewers who manufacture fewer than 2,000 barrels of malt liquor in a year $ 150

If a business licensed under this section is destroyed, or damaged to the extent that it cannot be carried on, or if it ceases because of the death or illness of the licensee, the commissioner may refund the license fee for the balance of the license period to the licensee or to the licensee's estate.

Sec. 2. Minnesota Statutes 2004, section 340A.404, subdivision 2, is amended to read:

Subd. 2. [SPECIAL PROVISION; CITY OF MINNEAPOLIS.] (a) The city of Minneapolis may issue an on-sale intoxicating liquor

license to the Guthrie Theater, the Cricket Theatre, the Orpheum Theatre, the State Theatre, and the Historic Pantages Theatre, notwithstanding the limitations of law, or local ordinance, or charter provision relating to zoning or school or church distances. The licenses authorize sales on all days of the week to holders of tickets for performances presented by the theaters and to members of the nonprofit corporations holding the licenses and to their guests.

(b) The city of Minneapolis may issue an intoxicating liquor license to 510 Groveland Associates, a Minnesota cooperative, for use by a restaurant on the premises owned by 510 Groveland Associates, notwithstanding limitations of law, or local ordinance, or charter provision.

(c) The city of Minneapolis may issue an on-sale intoxicating liquor license to Zuhrah Shrine Temple for use on the premises owned by Zuhrah Shrine Temple at 2540 Park Avenue South in Minneapolis, and to the American Swedish Institute for use on the premises owned by the American Swedish Institute at 2600 Park Avenue South, notwithstanding limitations of law, or local ordinances, or charter provision relating to zoning or school or church distances.

(d) The city of Minneapolis may issue an on-sale intoxicating liquor license to the American Association of University Women, Minneapolis branch, for use on the premises owned by the American Association of University Women, Minneapolis branch, at 2115 Stevens Avenue South in Minneapolis, notwithstanding limitations of law, or local ordinances, or charter provisions relating to zoning or school or church distances.

(e) The city of Minneapolis may issue an on-sale wine license and an on-sale 3.2 percent malt liquor license to a restaurant located at 5000 Penn Avenue South, and an on-sale wine license and an on-sale malt liquor license to a restaurant located at 1931 Nicollet Avenue South, notwithstanding any law or local ordinance or charter provision.

(f) The city of Minneapolis may issue an on-sale wine

license and an on-sale malt liquor license to the Brave New Workshop Theatre located at 3001 Hennepin Avenue South, the Theatre de la Jeune Lune, the Illusion Theatre located at 528 Hennepin Avenue South, the Hollywood Theatre located at 2815 Johnson Street Northeast, the Loring Playhouse located at 1633 Hennepin Avenue South, the Jungle Theater located at 2951 Lyndale Avenue South, Brave New Institute located at 2605 Hennepin Avenue South, the Guthrie Lab located at 700 North First Street, and the Southern Theatre located at 1420 Washington Avenue South, notwithstanding any law or local ordinance or charter provision. The license authorizes sales on all days of the week.

(g) The city of Minneapolis may issue an on-sale intoxicating liquor license to University Gateway Corporation, a Minnesota nonprofit corporation, for use by a restaurant or catering operator at the building owned and operated by the University Gateway Corporation on the University of Minnesota campus, notwithstanding limitations of law, or local ordinance or charter provision. The license authorizes sales on all days of the week.

(h) The city of Minneapolis may issue an on-sale intoxicating liquor license to the Guthrie Theater's concessionaire or operator for a restaurant and catering operator on the premises of the Guthrie Theater, notwithstanding limitations of law, local ordinance, or charter provisions. The license authorizes sales on all days of the week.

[EFFECTIVE DATE.] This section is effective the day following final enactment.

Sec. 3. Minnesota Statutes 2004, section 340A.418, is amended to read:

340A.418 [WINE TASTINGS.]

Subdivision 1. [DEFINITION.] For purposes of this section, a "wine tasting" is an event ~~of not more than four hours' duration~~ at which persons pay a fee or donation to participate, and are allowed to consume wine by the glass without paying a separate charge for each glass.

Subd. 2. [TASTINGS AUTHORIZED.] (a) A charitable, religious, or other nonprofit organization may conduct a wine tasting of not more than four hours duration on premises the organization owns or leases or has use donated to it, or on the licensed premises of a holder of an on-sale intoxicating liquor license that is not a temporary license, if the organization holds a temporary on-sale intoxicating liquor license under section 340A.404, subdivision 10, and complies with this section. An organization holding a temporary license may be assisted in conducting the wine tasting by another nonprofit organization.

(b) An organization that conducts a wine tasting under this section may use the net proceeds from the wine tasting only for:

(1) the organization's primary nonprofit purpose; or

(2) donation to another nonprofit organization assisting in the wine tasting, if the other nonprofit organization uses the donation only for that organization's primary nonprofit purpose.

(c) No wine at a wine tasting under this section may be sold, or orders taken, for off-premises consumption.

(d) Notwithstanding any other law, an organization may purchase or otherwise obtain wine for a wine tasting conducted under this section from a wholesaler licensed to sell wine, and the wholesaler may sell or give wine to an organization for a wine tasting conducted under this section and may provide personnel to assist in the wine tasting. A wholesaler who sells or gives wine to an organization for a wine tasting under this section must deliver the wine directly to the location where the wine tasting is conducted.

(e) This section does not prohibit or restrict a wine tasting that is:

(1) located on on-sale premises where no charitable organization is participating; or

(2) located on on-sale premises where the proceeds are for a designated charity but where the tasting is primarily for educational purposes.

(f) The four-hour limitation specified in paragraph (a)

shall not apply to a wine tasting at a convention of fine wine and gourmet food exhibitors, provided the convention has at least 100 exhibitors and takes place over not more than three days.

Sec. 4. [340A.5035] [MANDATORY PENALTIES AND COMPLIANCE CHECKS; SALE TO PERSONS UNDER AGE 21.]

(a) The authority issuing a retail license or operating a municipal liquor store must impose at a minimum the following civil penalties:

(1) for a first violation of section 340A.503 within a two-year period at the same location, $500 or training of establishment managers and servers approved by the authority, or both;

(2) for a second violation of section 340A.503 within a two-year period at the same location, $750;

(3) for a third violation of section 340A.503 within a two-year period at the same location, $750 plus a three-day suspension of the violator's retail license or three-day shutdown of the municipal liquor store; and

(4) for a fourth violation of section 340A.503 within a two-year period at the same location, the authority must revoke the violator's retail license or shut down the municipal liquor store.

(b) The commissioner may impose the penalties under paragraph (a) if the commissioner determines that the licensing authority or operator of the municipal liquor store has, after a reasonable period of time, failed to impose the penalties when required to do so under that paragraph.

(c) No suspension or penalty may take effect until the licensee has been given an opportunity for a hearing as provided in section 340A.415.

(d) After a violation of section 340A.503 is found, the authority must perform a compliance check on the violating retail license holder or municipal liquor store within 90 days of the violation.

(e) An authority issuing a retail license or operating a

municipal liquor store under this chapter must complete at least two compliance checks per year on each retail license holder or municipal liquor store to ensure compliance with the provisions of this chapter.

Sec. 5. Minnesota Statutes 2004, section 340A.504, subdivision 1, is amended to read:

Subdivision 1. [3.2 PERCENT MALT LIQUOR.] No sale of 3.2 percent malt liquor may be made between 2:00 a.m. and 8:00 a.m. on the days of Monday through Saturday, nor between 2:00 a.m. and ~~12:00 noon~~ 10:00 a.m. on Sunday~~, provided that an establishment located on land owned by the Metropolitan Sports Commission, or the sports arena for which one or more licenses have been issued under section 340A.404, subdivision 2, paragraph (c), may sell 3.2 percent malt liquor between 10:00 a.m. and 12:00 noon on a Sunday on which a sports or other event is scheduled to begin at that location on or before 1:00 p.m. of that day~~.

Sec. 6. Minnesota Statutes 2004, section 340A.504, subdivision 3, is amended to read:

Subd. 3. [INTOXICATING LIQUOR; SUNDAY SALES; ON-SALE.] (a) A restaurant, club, bowling center, or hotel with a seating capacity for at least 30 persons and which holds an on-sale intoxicating liquor license may sell intoxicating liquor for consumption on the premises in conjunction with the sale of food between the hours of ~~12:00 noon~~ 10:00 a.m. on Sundays and 2:00 a.m. on Mondays.

(b) ~~The governing body of a municipality may after one public hearing by ordinance permit a restaurant, hotel, bowling center, or club to sell alcoholic beverages for consumption on the premises in conjunction with the sale of food between the hours of 10:00 a.m. on Sundays and 2:00 a.m. on Mondays, provided that the licensee is in conformance with the Minnesota Clean Air Act.~~

~~(c)~~ An establishment serving intoxicating liquor on Sundays must obtain a Sunday license. The license must be issued by the governing body of the municipality for a period of one year, and

the fee for the license may not exceed $200.

~~(d)~~ (c) A city may issue a Sunday intoxicating liquor license only if authorized to do so by the voters of the city voting on the question at a general or special election. A county may issue a Sunday intoxicating liquor license in a town only if authorized to do so by the voters of the town as provided in paragraph ~~(e)~~ (d). A county may issue a Sunday intoxicating liquor license in unorganized territory only if authorized to do so by the voters of the election precinct that contains the licensed premises, voting on the question at a general or special election.

~~(e)~~ (d) An election conducted in a town on the question of the issuance by the county of Sunday sales licenses to establishments located in the town must be held on the day of the annual election of town officers.

~~(f)~~ (e) Voter approval is not required for licenses issued by the Metropolitan Airports Commission or common carrier licenses issued by the commissioner. Common carriers serving intoxicating liquor on Sunday must obtain a Sunday license from the commissioner at an annual fee of $50, plus $20 for each duplicate.

Sec. 7. Minnesota Statutes 2004, section 340A.504, subdivision 4, is amended to read:

Subd. 4. [INTOXICATING LIQUOR; OFF-SALE.] No sale of intoxicating liquor may be made by an off-sale licensee:

(1) on Sundays;

(2) before 8:00 a.m. or after 10:00 p.m. on Monday through Saturday;

~~(3) after 10:00 p.m. on Monday through Saturday at an establishment located in a city other than a city of the first class or within a city located within 15 miles of a city of the first class in the same county;~~

~~(4) after 8:00 p.m. on Monday through Thursday and after 10:00 p.m. on Friday and Saturday at an establishment located in a city of the first class or within a city located within 15 miles of a city of the first class in the same county, provided~~

~~that an establishment may sell intoxicating liquor until 10:00 p.m. on December 31 and July 3, and on the day preceding Thanksgiving day, unless otherwise prohibited under clause (1);~~

~~(5)~~ on Thanksgiving Day;

~~(6)~~ (4) on Christmas Day, December 25; or

~~(7)~~ (5) after 8:00 p.m. on Christmas Eve, December 24.

Sec. 8. Laws 2003, chapter 126, section 28, is amended to read:

Sec. 28. [ELKO SPEEDWAY; ON-SALE LICENSE.]

Notwithstanding Minnesota Statutes, section 340A.404, subdivision 1, the city of Elko may issue an on-sale intoxicating liquor license to the Elko Speedway in addition to the number authorized by law. The license may authorize sales ~~only~~ both to persons attending ~~racing~~ any and all events, and sales in a restaurant/bar/banquet facility, at the speedway. The license authorizes sales on all days of the week. All provisions of Minnesota Statutes, chapter 340A, not inconsistent with this provision, apply to the license authorized under this section. The license may be issued for a space that is not compact and contiguous, provided that the licensed premises may include only the space within the fenced ~~grandstand~~ area as described in the approved license application.

[EFFECTIVE DATE.] This section is effective upon approval by the Elko City Council and compliance with Minnesota Statutes, section 645.021.

Sec. 9. [CITY OF EDEN PRAIRIE; ON-SALE LICENSE.]

Notwithstanding any law, local ordinance, or charter provision, the city of Eden Prairie may issue an on-sale intoxicating liquor license to any entity holding an operating food service contract with the city for the operation of the cafeteria, for use by the entity at the premises owned by the city of Eden Prairie, at 8080 Mitchell Road in Eden Prairie. The license authorizes sales on all days of the week to persons attending special events in the cafeteria. The licensee may not dispense intoxicating liquor to any person attending or participating in an amateur athletic event held on the premises

unless such dispensing is authorized by resolution of the city council. The license authorized by this subdivision may be issued for space that is not compact and contiguous, provided that all such space is within the City Center building and is included in the description of the licensed premises on the approved license application.

[EFFECTIVE DATE.] This section is effective the day following final enactment.

Sec. 10. [MANKATO; ON-SALE INTOXICATING LIQUOR LICENSE.]

The city of Mankato may issue an on-sale intoxicating liquor license to the premises known as the Midwest Wireless Civic Center. The license authorizes sales on all days of the week to persons attending events at the center. All provisions of Minnesota Statutes, chapter 340A, not inconsistent with this section, apply to the license authorized under this section.

[EFFECTIVE DATE.] This section is effective the day following final enactment.

Sec. 11. [OFF-SALE INTOXICATING LIQUOR LICENSE; MILLE LACS COUNTY.]

Notwithstanding Minnesota Statutes, section 340A.405, subdivision 2, paragraph (e), the Mille Lacs County Board may issue an off-sale intoxicating liquor license to an exclusive liquor store located in Eastside Township. All other provisions of Minnesota Statutes, chapter 340A, not inconsistent with this section, apply to the license authorized under this section.

[EFFECTIVE DATE.] This section is effective the day following final enactment."

Amend the title as follows:

Page 1, line 6, after the semicolon, insert "regulating wine tastings; providing minimum administrative penalties for sales to underage persons; providing for uniform off-sale hours statewide; regulating Sunday on-sales; authorizing certain on-sale licenses;"

Page 1, line 7, delete "section" and insert "sections" and after "6" insert "; 340A.404, subdivision 2; 340A.418; 340A.504, subdivisions 1, 3, 4; Laws 2003 chapter 126, section 28;

proposing coding for new law in Minnesota Statutes, chapter 340A"

And when so amended that the bill be recommended to pass and be referred to the full committee.

.....
(Subcommittee Chair)

March 14, 2005.....
(Date of Subcommittee action)

Senator pappas moves to amend the Report of the Subcommittee on Liquor (SS0664SUB1) to S.F. No. 664 as follows:

Page 9, after line 25, insert:

"Sec. 9. [CITY OF DULUTH; ON-SALE LICENSE.]

Notwithstanding any other law, local ordinance, or charter provision, the city of Duluth may issue an on-sale intoxicating liquor license for the premises known and used as the Enger Park golf course, or for any portion of the premises as described in the approved license application. The license may be issued to the city or to any person or corporation under contract or agreement with the city with respect to operation of the golf course. All provisions of Minnesota Statutes, chapter 340A, not inconsistent herewith, apply to the license authorized under this section.

[EFFECTIVE DATE.] This section is effective the day following final enactment."

Renumber the sections in sequence and correct the internal references

Amend the title accordingly

CERTIFIED COPY OF RESOLUTION OF THE CITY COUNCIL OF THE CITY OF DULUTH, MINNESOTA

RESOLUTION 05-0221 ADOPTED: MARCH 28, 2005

BY COUNCILOR STEWART:

RESOLVED, that the Duluth City Council hereby memorializes the Duluth delegation to the state legislature to secure passage of special legislation authorizing the Duluth City Council to issue an intoxicating on sale liquor license for use on premises known as the Enger Golf Course.

Resolution 05-0221 was unanimously adopted.

Approved March 28, 2005

HERB W. BERGSON, Mayor

I, JEFFREY J. COX, city clerk of the city of Duluth, Minnesota, do hereby certify that I have compared the foregoing resolution passed by the city council on the 28th day of March, 2005, with the original in my custody as city clerk of said city, and that the same is a true and correct transcript therefrom.

IN WITNESS WHEREOF, I have hereunto set my hand and affixed the corporate seal of said city of Duluth, this 29th day of March, 2005.

JEFFREY J. COX
City Clerk

by _____
Assistant

CITY OF DULUTH, MINNESOTA

Senator Scheid from the Committee on Commerce, to which was referred

S.F. No. 664: A bill for an act relating to alcoholic beverages; allowing a brewer who manufactures beer on the premises where the brewer also holds an on-sale intoxicating liquor license to use wort produced outside Minnesota under certain circumstances; amending Minnesota Statutes 2004, section 340A.301, subdivision 6.

Reports the same back with the recommendation that the bill be amended as follows:

Delete everything after the enacting clause and insert:

"Section 1. Minnesota Statutes 2004, section 340A.301, subdivision 6, is amended to read:

Subd. 6. [FEES.] The annual fees for licenses under this section are as follows:

(a) Manufacturers (except as provided in clauses (b) and (c))	$15,000
Duplicates	$ 3,000
(b) Manufacturers of wines of not more than 25 percent alcohol by volume	$ 500
(c) Brewers other than those described in clauses (d) and (i)	$ 2,500
(d) Brewers who also hold one or more retail on-sale licenses and who manufacture fewer than 3,500 barrels of malt liquor in a year, at any one licensed premises, ~~using only wort produced in Minnesota,~~ the entire production of which is solely for consumption on tap on the licensed premises or for off-sale from that licensed premises. A brewer licensed under this clause must obtain a separate license for each licensed premises where the brewer brews malt liquor. A brewer licensed under this clause may not be licensed as an importer under this chapter	$ 500
(e) Wholesalers (except as provided in	

	clauses (f), (g), and (h))	$15,000
	Duplicates	$ 3,000
(f)	Wholesalers of wines of not more than 25 percent alcohol by volume	$ 2,000
(g)	Wholesalers of intoxicating malt liquor	$ 600
	Duplicates	$ 25
(h)	Wholesalers of 3.2 percent malt liquor	$ 10
(i)	Brewers who manufacture fewer than 2,000 barrels of malt liquor in a year	$ 150

If a business licensed under this section is destroyed, or damaged to the extent that it cannot be carried on, or if it ceases because of the death or illness of the licensee, the commissioner may refund the license fee for the balance of the license period to the licensee or to the licensee's estate.

Sec. 2. Minnesota Statutes 2004, section 340A.301, subdivision 7, is amended to read:

Subd. 7. [INTEREST IN OTHER BUSINESS.] (a) Except as provided in this subdivision, a holder of a license as a manufacturer, brewer, importer, or wholesaler may not have any ownership, in whole or in part, in a business holding a retail intoxicating liquor or 3.2 percent malt liquor license. The commissioner may not issue a license under this section to a manufacturer, brewer, importer, or wholesaler if a retailer of intoxicating liquor has a direct or indirect interest in the manufacturer, brewer, importer, or wholesaler. A manufacturer or wholesaler of intoxicating liquor may use or have property rented for retail intoxicating liquor sales only if the manufacturer or wholesaler has owned the property continuously since November 1, 1933. A retailer of intoxicating liquor may not use or have property rented for the manufacture or wholesaling of intoxicating liquor.

(b) A brewer licensed under subdivision 6, clause (d), may be issued an on-sale intoxicating liquor or 3.2 percent malt liquor license by a municipality for a restaurant operated in

the place of manufacture. Notwithstanding section 340A.405, a brewer who holds an on-sale license issued pursuant to this paragraph may, with the approval of the commissioner, be issued a license by a municipality for off-sale of malt liquor produced and packaged on the licensed premises. Off-sale of malt liquor shall be limited to the legal hours for off-sale at exclusive liquor stores in the jurisdiction in which the brewer is located, and the malt liquor sold off-sale must be removed from the premises before the applicable off-sale closing time at exclusive liquor stores. The malt liquor shall be packaged in 64-ounce containers commonly known as "growlers." The containers shall bear a twist-type closure, cork, stopper, or plug. At the time of the sale, a paper or plastic adhesive band, strip, or sleeve shall be applied to the container and extend over the top of the twist-type closure, cork, stopper, or plug forming a seal that must be broken upon opening of the container. The adhesive band, strip, or sleeve shall bear the name and address of the brewer. The containers shall be identified as malt liquor, contain the name of the malt liquor, bear the name and address of the brewer selling the malt liquor, and shall be considered intoxicating liquor unless the alcoholic content is labeled as otherwise in accordance with the provisions of Minnesota Rules, part 7515.1100. A brewer's total retail sales at on- or off-sale under this paragraph may not exceed 3,500 barrels per year, provided that off-sales may not total more than ~~50 percent of the brewer's production or~~ 500 barrels~~, whichever is less~~. A brewer licensed under subdivision 6, clause (d), may hold or have an interest in other retail on-sale licenses, but may not have an ownership interest in whole or in part, or be an officer, director, agent, or employee of, any other manufacturer, brewer, importer, or wholesaler, or be an affiliate thereof whether the affiliation is corporate or by management, direction, or control. Notwithstanding this prohibition, a brewer licensed under subdivision 6, clause (d), may be an affiliate or subsidiary company of a brewer licensed in Minnesota or elsewhere if that brewer's only manufacture of

malt liquor is:

(i) manufacture licensed under subdivision 6, clause (d);

(ii) manufacture in another state for consumption exclusively in a restaurant located in the place of manufacture; or

(iii) manufacture in another state for consumption primarily in a restaurant located in or immediately adjacent to the place of manufacture if the brewer was licensed under subdivision 6, clause (d), on January 1, 1995.

(c) Except as provided in subdivision 7a, no brewer as defined in subdivision 7a or importer may have any interest, in whole or in part, directly or indirectly, in the license, business, assets, or corporate stock of a licensed malt liquor wholesaler.

Sec. 3. Minnesota Statutes 2004, section 340A.404, subdivision 2, is amended to read:

Subd. 2. [SPECIAL PROVISION; CITY OF MINNEAPOLIS.] (a) The city of Minneapolis may issue an on-sale intoxicating liquor license to the Guthrie Theater, the Cricket Theatre, the Orpheum Theatre, the State Theatre, and the Historic Pantages Theatre, notwithstanding the limitations of law, or local ordinance, or charter provision relating to zoning or school or church distances. The licenses authorize sales on all days of the week to holders of tickets for performances presented by the theaters and to members of the nonprofit corporations holding the licenses and to their guests.

(b) The city of Minneapolis may issue an intoxicating liquor license to 510 Groveland Associates, a Minnesota cooperative, for use by a restaurant on the premises owned by 510 Groveland Associates, notwithstanding limitations of law, or local ordinance, or charter provision.

(c) The city of Minneapolis may issue an on-sale intoxicating liquor license to Zuhrah Shrine Temple for use on the premises owned by Zuhrah Shrine Temple at 2540 Park Avenue South in Minneapolis, and to the American Swedish Institute for use on the premises owned by the American Swedish Institute at

2600 Park Avenue South, notwithstanding limitations of law, or local ordinances, or charter provision relating to zoning or school or church distances.

(d) The city of Minneapolis may issue an on-sale intoxicating liquor license to the American Association of University Women, Minneapolis branch, for use on the premises owned by the American Association of University Women, Minneapolis branch, at 2115 Stevens Avenue South in Minneapolis, notwithstanding limitations of law, or local ordinances, or charter provisions relating to zoning or school or church distances.

(e) The city of Minneapolis may issue an on-sale wine license and an on-sale 3.2 percent malt liquor license to a restaurant located at 5000 Penn Avenue South, and an on-sale wine license and an on-sale malt liquor license to a restaurant located at 1931 Nicollet Avenue South, notwithstanding any law or local ordinance or charter provision.

(f) The city of Minneapolis may issue an on-sale wine license and an on-sale malt liquor license to the Brave New Workshop Theatre located at 3001 Hennepin Avenue South, the Theatre de la Jeune Lune, the Illusion Theatre located at 528 Hennepin Avenue South, the Hollywood Theatre located at 2815 Johnson Street Northeast, the Loring Playhouse located at 1633 Hennepin Avenue South, the Jungle Theater located at 2951 Lyndale Avenue South, Brave New Institute located at 2605 Hennepin Avenue South, the Guthrie Lab located at 700 North First Street, and the Southern Theatre located at 1420 Washington Avenue South, notwithstanding any law or local ordinance or charter provision. The license authorizes sales on all days of the week.

(g) The city of Minneapolis may issue an on-sale intoxicating liquor license to University Gateway Corporation, a Minnesota nonprofit corporation, for use by a restaurant or catering operator at the building owned and operated by the University Gateway Corporation on the University of Minnesota campus, notwithstanding limitations of law, or local ordinance

or charter provision. The license authorizes sales on all days of the week.

(h) The city of Minneapolis may issue an on-sale intoxicating liquor license to the Guthrie Theater's concessionaire or operator for a restaurant and catering operator on the premises of the Guthrie Theater, notwithstanding limitations of law, local ordinance, or charter provisions. The license authorizes sales on all days of the week.

[EFFECTIVE DATE.] This section is effective the day following final enactment.

Sec. 4. Minnesota Statutes 2004, section 340A.418, is amended to read:

340A.418 [WINE TASTINGS.]

Subdivision 1. [DEFINITION.] For purposes of this section, a "wine tasting" is an event ~~of not more than four hours' duration~~ at which persons pay a fee or donation to participate, and are allowed to consume wine by the glass without paying a separate charge for each glass.

Subd. 2. [TASTINGS AUTHORIZED.] (a) A charitable, religious, or other nonprofit organization may conduct a wine tasting of not more than four hours duration on premises the organization owns or leases or has use donated to it, or on the licensed premises of a holder of an on-sale intoxicating liquor license that is not a temporary license, if the organization holds a temporary on-sale intoxicating liquor license under section 340A.404, subdivision 10, and complies with this section. An organization holding a temporary license may be assisted in conducting the wine tasting by another nonprofit organization.

(b) An organization that conducts a wine tasting under this section may use the net proceeds from the wine tasting only for:

(1) the organization's primary nonprofit purpose; or

(2) donation to another nonprofit organization assisting in the wine tasting, if the other nonprofit organization uses the donation only for that organization's primary nonprofit purpose.

(c) No wine at a wine tasting under this section may be

sold, or orders taken, for off-premises consumption.

(d) Notwithstanding any other law, an organization may purchase or otherwise obtain wine for a wine tasting conducted under this section from a wholesaler licensed to sell wine, and the wholesaler may sell or give wine to an organization for a wine tasting conducted under this section and may provide personnel to assist in the wine tasting. A wholesaler who sells or gives wine to an organization for a wine tasting under this section must deliver the wine directly to the location where the wine tasting is conducted.

(e) This section does not prohibit or restrict a wine tasting that is:

(1) located on on-sale premises where no charitable organization is participating; or

(2) located on on-sale premises where the proceeds are for a designated charity but where the tasting is primarily for educational purposes.

(f) The four-hour limitation specified in paragraph (a) shall not apply to a wine tasting at a convention of fine wine and gourmet food exhibitors, provided the convention has at least 100 exhibitors and takes place over not more than three days.

Sec. 5. Minnesota Statutes 2004, section 340A.504, subdivision 1, is amended to read:

Subdivision 1. [3.2 PERCENT MALT LIQUOR.] No sale of 3.2 percent malt liquor may be made between 2:00 a.m. and 8:00 a.m. on the days of Monday through Saturday, nor between 2:00 a.m. and ~~12:00 noon~~ 10:00 a.m. on Sunday~~, provided that an establishment located on land owned by the Metropolitan Sports Commission, or the sports arena for which one or more licenses have been issued under section 340A.404, subdivision 2, paragraph (c), may sell 3.2 percent malt liquor between 10:00 a.m. and 12:00 noon on a Sunday on which a sports or other event is scheduled to begin at that location on or before 1:00 p.m. of that day~~.

Sec. 6. Minnesota Statutes 2004, section 340A.504,

subdivision 3, is amended to read:

Subd. 3. [INTOXICATING LIQUOR; SUNDAY SALES; ON-SALE.] (a) A restaurant, club, bowling center, or hotel with a seating capacity for at least 30 persons and which holds an on-sale intoxicating liquor license may sell intoxicating liquor for consumption on the premises in conjunction with the sale of food between the hours of ~~12:00 noon~~ 10:00 a.m. on Sundays and 2:00 a.m. on Mondays.

(b) ~~The governing body of a municipality may after one public hearing by ordinance permit a restaurant, hotel, bowling center, or club to sell alcoholic beverages for consumption on the premises in conjunction with the sale of food between the hours of 10:00 a.m. on Sundays and 2:00 a.m. on Mondays, provided that the licensee is in conformance with the Minnesota Clean Air Act.~~

~~(c)~~ An establishment serving intoxicating liquor on Sundays must obtain a Sunday license. The license must be issued by the governing body of the municipality for a period of one year, and the fee for the license may not exceed $200.

~~(d)~~ (c) A city may issue a Sunday intoxicating liquor license only if authorized to do so by the voters of the city voting on the question at a general or special election. A county may issue a Sunday intoxicating liquor license in a town only if authorized to do so by the voters of the town as provided in paragraph ~~(e)~~ (d). A county may issue a Sunday intoxicating liquor license in unorganized territory only if authorized to do so by the voters of the election precinct that contains the licensed premises, voting on the question at a general or special election.

~~(e)~~ (d) An election conducted in a town on the question of the issuance by the county of Sunday sales licenses to establishments located in the town must be held on the day of the annual election of town officers.

~~(f)~~ (e) Voter approval is not required for licenses issued by the Metropolitan Airports Commission or common carrier licenses issued by the commissioner. Common carriers serving

intoxicating liquor on Sunday must obtain a Sunday license from the commissioner at an annual fee of $50, plus $20 for each duplicate.

Sec. 7. Minnesota Statutes 2004, section 340A.504, subdivision 4, is amended to read:

Subd. 4. [INTOXICATING LIQUOR; OFF-SALE.] No sale of intoxicating liquor may be made by an off-sale licensee:

(1) on Sundays;

(2) before 8:00 a.m. or after 10:00 p.m. on Monday through Saturday;

~~(3) after 10:00 p.m. on Monday through Saturday at an establishment located in a city other than a city of the first class or within a city located within 15 miles of a city of the first class in the same county;~~

~~(4) after 8:00 p.m. on Monday through Thursday and after 10:00 p.m. on Friday and Saturday at an establishment located in a city of the first class or within a city located within 15 miles of a city of the first class in the same county, provided that an establishment may sell intoxicating liquor until 10:00 p.m. on December 31 and July 3, and on the day preceding Thanksgiving day, unless otherwise prohibited under clause (1);~~

~~(5)~~ on Thanksgiving Day;

~~(6)~~ (4) on Christmas Day, December 25; or

~~(7)~~ (5) after 8:00 p.m. on Christmas Eve, December 24.

Sec. 8. Laws 2000, chapter 440, section 10, is amended to read:

Sec. 10. [WINE LICENSE; MAIN STREET STAGE THEATRE.]

The city of Anoka may issue an on-sale wine and malt liquor license to the Lyric Arts Company of Anoka, Inc. for the Main Street Stage Theatre. The license authorizes sales of wine and malt liquor on all days of the week to holders of tickets for performances at the theater. All provisions of Minnesota Statutes, chapter 340A, not inconsistent with this section, apply to the license authorized under this section.

[EFFECTIVE DATE.] This section is effective on approval by the Anoka City Council and compliance with Minnesota Statutes,

section 645.021.

Sec. 9. Laws 2003, chapter 126, section 28, is amended to read:

Sec. 28. [ELKO SPEEDWAY; ON-SALE LICENSE.]

Notwithstanding Minnesota Statutes, section 340A.404, subdivision 1, the city of Elko may issue an on-sale intoxicating liquor license to the Elko Speedway in addition to the number authorized by law. The license may authorize sales ~~only~~ both to persons attending ~~racing~~ any and all events, and sales in a restaurant/bar/banquet facility, at the speedway. The license authorizes sales on all days of the week. All provisions of Minnesota Statutes, chapter 340A, not inconsistent with this provision, apply to the license authorized under this section. The license may be issued for a space that is not compact and contiguous, provided that the licensed premises may include only the space within the fenced ~~grandstand~~ area as described in the approved license application.

[EFFECTIVE DATE.] This section is effective upon approval by the Elko City Council and compliance with Minnesota Statutes, section 645.021.

Sec. 10. [CITY OF CALEDONIA; LIQUOR LICENSE.]

Notwithstanding any other law, the city of Caledonia may issue an on-sale intoxicating liquor license to Caledonia Area Community Charities, Inc., for the Four Seasons Center in Caledonia. The license authorizes the licensee to dispense intoxicating liquor only to persons attending events at the center. All provisions of Minnesota Statutes, chapter 340A, not inconsistent with this section, apply to the license authorized under this section.

[EFFECTIVE DATE.] This section is effective the day following final enactment.

Sec. 11. [DETROIT LAKES; ON-SALE.]

Notwithstanding Minnesota Statutes, section 340A.404, subdivision 1, the city of Detroit Lakes may issue an on-sale intoxicating liquor license, or an on-sale wine license and an on-sale malt liquor license, to the Castaway Inn and Resort

located at 1200 East Shore Drive, notwithstanding any law, local ordinance, or charter provision. The license may authorize sales only to persons that are registered guests at the lodging establishment, their invitees, or persons attending the spa, a conference, a meeting, or other events at the lodging establishment. The license authorizes sales on all days of the week.

Sec. 12. [CITY OF DULUTH; ON-SALE LICENSE.]

Notwithstanding any other law, local ordinance, or charter provision, the city of Duluth may issue an on-sale intoxicating liquor license for the premises known and used as the Enger Park golf course, or for any portion of the premises as described in the approved license application. The license may be issued to the city or to any person or corporation under contract or agreement with the city with respect to operation of the golf course. All provisions of Minnesota Statutes, chapter 340A, not inconsistent herewith, apply to the license authorized under this section.

[EFFECTIVE DATE.] This section is effective the day following final enactment.

Sec. 13. [CITY OF EDEN PRAIRIE; ON-SALE LICENSE.]

Notwithstanding any law, local ordinance, or charter provision, the city of Eden Prairie may issue an on-sale intoxicating liquor license to any entity holding an operating food service contract with the city for the operation of the cafeteria, for use by the entity at the premises owned by the city of Eden Prairie, at 8080 Mitchell Road in Eden Prairie. The license authorizes sales on all days of the week to persons attending special events in the cafeteria. The licensee may not dispense intoxicating liquor to any person attending or participating in an amateur athletic event held on the premises unless such dispensing is authorized by resolution of the city council. The license authorized by this subdivision may be issued for space that is not compact and contiguous, provided that all such space is within the City Center building and is included in the description of the licensed premises on the

approved license application.

[EFFECTIVE DATE.] This section is effective the day following final enactment.

Sec. 14. [MANKATO; ON-SALE INTOXICATING LIQUOR LICENSE.]

The city of Mankato may issue an on-sale intoxicating liquor license to the premises known as the Midwest Wireless Civic Center. The license authorizes sales on all days of the week to persons attending events at the center. All provisions of Minnesota Statutes, chapter 340A, not inconsistent with this section, apply to the license authorized under this section.

[EFFECTIVE DATE.] This section is effective the day following final enactment.

Sec. 15. [OFF-SALE INTOXICATING LIQUOR LICENSE; MILLE LACS COUNTY.]

Notwithstanding Minnesota Statutes, section 340A.405, subdivision 2, paragraph (e), the Mille Lacs County Board may issue an off-sale intoxicating liquor license to an exclusive liquor store located in Eastside Township. All other provisions of Minnesota Statutes, chapter 340A, not inconsistent with this section, apply to the license authorized under this section.

[EFFECTIVE DATE.] This section is effective the day following final enactment."

Delete the title and insert:

"A bill for an act relating to alcoholic beverages; modifying brewpub regulations; regulating wine tastings; providing for uniform off-sale hours statewide; regulating Sunday on-sales; authorizing certain on-sale licenses; amending Minnesota Statutes 2004, sections 340A.301, subdivisions 6, 7; 340A.404, subdivision 2; 340A.418; 340A.504, subdivisions 1, 3, 4; Laws 2000, chapter 440, section 10; Laws 2003, chapter 126, section 28."

And when so amended the bill do pass. Amendments adopted. Report adopted.

.....
(Committee Chair)

April 6, 2005.....
(Date of Committee recommendation)